MASTER EN SCIENCES INFORMATIQUES

Génération de carrés magiques et bimagiques à l'aide d'une méthode algébrique

Lacroix, Bruno

Award date:
2009

Facultés Universitaires Notre-Dame de la Paix, Namur
Faculté d'informatique.
Année académique 2008 - 2009

Génération de carrés magiques et bimagiques à l'aide d'une méthode algébrique

Bruno LACROIX

Mémoire présenté en vue de l'obtention du grade de licencié en informatique.

RESUME

Ce travail a pour but d'expliquer et d'implémenter une méthode algébrique permettant la génération de carrés magiques et bimagiques.
La terminologie concernant le domaine des carrés magiques est rappelée et les résultats principaux portant sur la bimagie sont exposés.
Les outils mathématiques nécessaires à la compréhension du travail sont fournis. Ceux-ci ont trait à l'algèbre des anneaux unitaires.
La méthode est présentée et une démonstration détaillée de sa correction est développée. Les différentes caractéristiques de la méthode - quant aux paramètres intervenant dans la génération des carrés (bi)magiques - sont étudiés. Il est ainsi argumenté que la méthode est plus générale que ce que ses auteurs soutiennent. Le nombre de carrés (bi)magiques générés s'en trouve donc grandement augmenté. Enfin, une implémentation logicielle est détaillée, qui utilise toute la méthode pour générer des carrés magiques et bimagiques pour les ordres inférieurs ou égaux à 25 auxquels elle s'applique.

MOTS CLES : Bimagie, Anneaux unitaires, Module libre

ABSTRACT

The purpose of this work is to explain et implement an algebric method allowing production of magical and bimagical squares.
The terminology related to the magical squares' domain is remainded and the major results concerning bimagic are provided.
Mathematical tools necessary for the understanding of this work are also provided. These ones are about algebra and unitary rings.
The method is presented and a detailed demonstration of its correction is developped. The various caracteristics of the method - as far as the parameters used in the production of (bi)magical squares are concerned – are examined. It is therefore argued that the method is more general than what the authors uphold. The amount of magical squares porduced becomes thus highly increased. Eventually, a software implementation is detailed, which uses the entire method to produce magical and bimagical squares for orders less than or equal to 25 which it applies.

KEY WORDS : Bimagic, Unitary Rings, Free Module

Table des matières

Remerciements

C'est assurément la partie la plus facile de ce travail, car je sais combien je dois à une série de personnes.

Tout d'abord, bien évidemment, au Professeur Jean-Paul Leclercq, promoteur de ce mémoire, pour sa disponibilité, ses conseils avisés dans l'élaboration du texte et ses nombreux encouragements.

Au Docteur Alexandre Jacques ensuite, co-promoteur, qui m'a généreusement fait profiter de sa connaissance approfondie du domaine des carrés magiques et a attiré mon attention sur ce secteur peu défriché des mathématiques.

Mes remerciements vont également à mon entourage qui m'a soutenu et n'a jamais cessé de me 'booster' pour que j'achève pleinement mon cursus universitaire.

Je pense d'abord à Alain, avec qui, les soirées passées à discuter de carrés magiques et de mathématique, furent, pour moi, l'occasion d'affiner ma pensée. Ses remarques judicieuses m'ont conduit à remanier certains passages de ce texte, qui sinon, aurait été trop indigeste.
Nous allons enfin nous retrouver sur un autre carré, magique également, l'échiquier de 64 cases !
Merci aussi à Diane, sa compagne, pour toute sa science psychologique à mon égard.

Je pense, bien sûr, à Myriam, mon épouse, qui durant toutes ces longues années d'études, a cru à ma capacité de rédiger ce mémoire et a su m'en convaincre. Grâce à elle, les moments de doutes furent surmontés et son soutien m'apporta, plus sans doute que je ne l'ai montré, un réconfort immense. Mon Coeur, merci pour tout !

Je remercie mes enfants, Louise et Jules, pour leur patiente attente de leur Papa, qui était plus souvent dans son bureau qu'à jouer avec eux. Ce n'était que partie remise...

Enfin, je remercie toutes celles et ceux qui de près ou de loin m'ont soutenu ou conseillé dans cette épreuve : Philippe, mes collègues de travail, mes parents, ma soeur et mon beauf', ...

Introduction

Les carrés magiques font l'objet d'études depuis des millénaires. Le présent mémoire s'inscrit dans cette lignée.

Originaires de Chine, les carrés magiques ont été étudiés par les civilisations indienne, perse, arabe avant de fasciner l'Europe du Moyen-Age. Une forte charge symbolique leur est associée à travers l'histoire ; différents cercles ésotériques conférant à ceux-ci des propriétés explicatives de la Nature.

Plusieurs mathématiciens, dont Pierre de Fermat (17^{eme}s.) et Léonard Euler(18^{eme}s.), s'y intéressèrent et en découvrirent de nombreuses propriétés. Ils élaborèrent, au cours des siècles, différents algorithmes pour générer des carrés magiques. Plus récemment (2005), une méthode algébrique générale a été développée par trois mathématiciens, Harm Derksen, Christian Eggermont et Arno van den Essen, travaillant respectivement au sein des Universités du Michigan et de Nijmegen. Le but de ce travail est d'expliquer et d'implémenter cette méthode.

En science, les carrés magiques sont utilisés dans des travaux de statistique et de génétique[1]. C'est dans ce dernier contexte d'étude que se situent les recherches du Docteur Alexandre Jacques, co-promoteur de ce travail.

En 2006-2007, le mémoire de Jean-Noël Leblanc [Leblanc 2007] portait sur la *magie simple*[2] d'ordre plus petit ou égal à 23. Jean-Noël Leblanc entendait fixer les valeurs des éléments diagonaux des carrés magiques générés. Il utilisait, pour ce faire, des méthodes méta-heuristiques de recherche opérationnelle.

Dans le cadre du présent travail, nous nous consacrerons à la génération de carrés *bimagiques*. Au cours d'une conversation avec Jean-Noël Leblanc, celui-ci nous avait fait part de ses essais infructueux pour générer des carrés bimagiques à partir de son approche.

C'est à la lecture de l'article [Multimagic Squares 2005] relatif à la multimagie des trois mathématiciens dont question supra qu'est venue l'idée d'une solution possible pour la génération de carrés bimagiques, du moins pour des ordres qui sont des carrés parfaits (9, 16, 25, ...). Ensuite, lors d'une discussion avec le Professeur J.P. Leclercq et le Docteur A.Jacques, une utilisation de cette méthode fut proposée afin d'étudier la *bimagie partielle* exploitable dans les recherches de ce dernier.

Considérant l'aspect technique de l'article en question, on comprendra que ce mémoire présente une connotation mathématique certaine.
C'est pour cette raison que l'on n'y a pas adjoint de glossaire à proprement parler. En effet, l'interdépendance des notions mobilisées aurait rapidement transformé celui-ci en un dictionnaire de mathématiques peu lisible. Toutefois, les chapitres un et deux éclaireront au besoin le lecteur sur les concepts au coeur du présent travail.

[1] le premier chapitre du mémoire de Jean-Noel Leblanc [Leblanc 2007] résume la manière dont les carrés magiques sont utilisés dans ces sciences.

[2] toute la terminologie concernant les carrés magiques sera donnée dans le prochain chapitre.

Le mémoire est articulé comme suit :

Dans le premier chapitre sera fixée la terminologie du domaine des carrés magiques et multimagiques, ainsi que des résultats connus d'impossibilité de l'existence de carrés bimagiques pour certains ordres.

Les outils mathématiques nécessaires à la compréhension de l'article mentionné ci-dessus seront introduits de manière progressive dans le deuxième chapitre. Partant de rappels de définition et de résultats bien connus, nous en arriverons à introduire des concepts d'algèbre supérieure. Ces résultats seront donnés sans démonstration, mais néanmoins explicités à l'aide d'exemples et de contre-exemples.

Le troisième chapitre est au coeur du mémoire puisqu'il s'agira d'exposer la méthode algébrique des trois auteurs. Celle-ci a pour résultat principal un théorème établissant la possibilité de construire des carrés multimagiques en utilisant des structures mathématiques spécifiques.
Afin de permettre une compréhension plus aisée au lecteur, et vu la densité de l'article, les définitions, lemmes et théorèmes seront également explicités à l'aide d'exemples, et les démonstrations y afférentes seront sensiblement plus développées que celles de l'article lui-même, tout en suivant le raisonnement des auteurs. On lèvera ce faisant une hypothèse trop forte émise par les auteurs dans la démonstration du théorème, ce qui nous permettra d'augmenter le nombre de possibilités lors de la génération des carrés.

Après ces deux chapitres assurément complexes d'un point de vue technique, il sera discuté dans un quatrième chapitre des choix concernant les paramètres intervenant dans la méthode. Il sera établi que certains ordres de carrés ne sont pas atteignables par celle-ci. Ce chapitre indiquera l'ordre de grandeur de la combinatoire des différents paramètres, dont il est d'ores et déjà précisé qu'il s'agit d'un très grand nombre. De ce fait, dans la pratique, des choix aléatoires de paramètres devront être faits.

Le cinquième chapitre sera consacré à l'implémentation effective de la méthode au travers d'un logiciel. L'architecture générale du programme ainsi que les principales structures de données utilisées seront détaillées. Certains algorithmes seront décrits. On donnera une estimation de la complexité algorithmique du programme.

Le chapitre suivant s'attaquera à un ordre particulier : l'ordre 7. Le Docteur A. Jacques est intéressé dans ses recherches par des résultats concernant la bimagie pour cet ordre. La méthode, et donc le programme, ne peuvent générer de carrés bimagiques à l'ordre 7 mais peuvent générer facilement un très grand nombre de carrés possèdant la magie simple. Ensuite les résultats produits seront classés en fonction du nombre d'éléments (lignes, colonnes, diagonales) ayant la somme bimagique. Les calculs donnant le nombre de combinaisons possibles seront faits.

Dans le septième et dernier chapitre, des conclusions seront tirées sur les avantages et inconvénients de la méthode. L'accent sera mis sur les possibilités d'amélioration future.

Chapitre 1

Carrés magiques - terminologie - résultats connus

Ce chapitre commence par fixer la terminologie du domaine des carrés magiques. Cette terminologie sera utilisée dans la suite du travail.

Ensuite, nous donnerons des résultats prouvés et conjecturés concernant la bimagie.

1.1 Définitions

1.1.1 Carré Magique

On appelle *carré magique*[1] un tableau carré contenant des nombres entiers tels que les sommes de toutes les lignes, de toutes les colonnes et des deux diagonales soient constantes.

On appelera *diagonale* du carré l'ensemble des éléments se trouvant sur la grande diagonale du carré, qui va du coin supérieur gauche au coin inférieur droit, et *contre-diagonale* l'ensemble des éléments se trouvant sur l'autre grande diagonale, du coin inférieur gauche au coin supérieur droit.

1.1.2 Ordre d'un carré

L'*ordre du carré* est le nombre d'éléments d'un côté du carré.

Exemple : voici un carré magique d'ordre 5 :

[1] En ce qui concerne l'histoire des carrés magiques, on consultera avec intérêt les ouvrages de René Descombes [Descombes 2000] et [Descombes 2004] ; cette dernière référence parlant plus généralement des carrés non spécifiquement magiques mais présentant beaucoup de propriétés . . .magiques !

Le fascicule du Docteur Alexandre Jacques [Jacques, Docteur A. 2008] contient également nombre d'éléments historiques concernant le sujet.

5	23	7	16	14
19	12	21	10	3
11	9	18	2	25
8	1	15	24	17
22	20	4	13	6

1.1.3 Carré normal

Un carré magique est dit *normal* si les nombres qu'il contient vont de 1 à $ordre^2$. L'exemple donné ci-dessus est un carré normal puisque les nombres vont de 1 à 25 (5^2). Dans ce travail, nous ne considérerons que des carrés magiques normaux.

1.1.4 Constante de magie simple

La somme constante d'un carré magique est appelée *constante de magie simple* du carré. Lorsque le carré est normal, elle est donnée par la formule

$$\frac{c(c^2+1)}{2} \text{ où } c \text{ est l'ordre du carré}$$

Dans l'exemple donné ci-dessus, on vérifie que la somme de chaque ligne (ou colonne ou diagonale) est égale à $5(5^2+1)/2 = 65$.

1.1.5 Carré bimagique

Un *carré bimagique* est un carré magique qui, lorsque l'on élève chacun de ses éléments au carré, reste magique (c'est-à-dire que la somme sur les lignes, colonnes et diagonales est une autre constante).

D'après [Site Multimagie], le premier carré bimagique (normal) date de 1890 et est dû au français G. Pfeffermann. Il est d'ordre 8 :

56	34	8	57	18	47	9	31
33	20	54	48	7	29	59	10
26	43	13	23	64	38	4	49
19	5	35	30	53	12	46	60
15	25	63	2	41	24	50	40
6	55	17	11	36	58	32	45
61	16	42	52	27	1	39	22
44	62	28	37	14	51	21	3

Le Docteur A. Jacques a travaillé sur ces carrés bimagiques de Pfeffermann et a pu déterminer une méthode lui permettant d'en construire d'autres. Voici, extrait d'un cahier personnel du Docteur Jacques, deux carrés bimagiques construits à l'aide de sa méthode. Il s'agit des carrés appelés O_3 et O_4 dans la nomenclature du Docteur Jacques[2].

[2]dans le cahier, les carrés sont composés des nombres de l'ensemble $\{0, \ldots, 63\}$. Ici, pour des raisons de cohérence avec le reste de notre travail, nous les avons 'translatés' pour que les valeurs soient comprises entre 1 et 64. On montre que cela ne change évidemment rien au caractère bimagique du carré.

24	13	39	62	41	52	26	3
27	2	44	49	38	63	21	16
1	28	51	42	61	40	15	22
14	23	64	37	50	43	4	25
36	57	18	11	32	5	46	55
47	54	29	8	19	10	33	60
53	48	6	31	12	17	59	34
58	35	9	20	7	30	56	45

24	27	41	38	55	60	10	5
29	18	36	47	62	49	3	16
50	61	15	4	17	30	48	35
59	56	6	9	28	23	37	42
12	7	64	51	34	45	22	25
1	14	53	58	43	40	31	20
39	44	19	32	13	2	57	54
46	33	26	21	8	11	52	63

Dans son cahier, le Docteur Jacques fait une analyse fouillée des propriétés de ces carrés de Pfeffermann. Entre autres, il indique que certains de ceux-ci ont des rangées tri-magiques[3].

1.1.6 Constante de bimagie

Cette nouvelle constante, la somme des carrés des éléments d'une ligne, colonne ou diagonale est appelée *constante de bimagie*. Dans le cas des carrés magiques normaux, cette constante se calcule par la formule :

$$\frac{c(2c^2+1)(c^2+1)}{6} \text{ où } c \text{ est l'ordre du carré}$$

Dans l'exemple ci-dessus, on vérifie bien que les sommes des lignes, colonnes et diagonales font $8(8^2+1)/2 = 260$ et si on élève les éléments au carré, on obtient le carré suivant

3136	1156	64	3249	324	2209	81	961
1089	400	2916	2304	49	841	3481	100
676	1849	169	529	4096	1144	16	2401
361	25	1225	900	2809	144	2116	3600
225	625	3969	4	1681	576	2500	1600
36	3025	289	121	1296	3364	1024	2025
3721	256	1764	2704	729	1	1521	484
1936	3844	784	1369	196	2601	441	9

dont les sommes sur les lignes, colonnes et diagonales font $8(2.8^2+1)(8^2+1)/6 = 11180$

Voici un exemple de carré bimagique d'ordre 9, généré, celui-ci, par notre programme :

40	77	6	25	35	72	55	11	48
17	54	61	74	3	37	32	69	22
66	19	29	51	58	14	9	43	80
36	70	26	12	46	56	78	4	41
1	38	75	67	23	33	52	62	18
59	15	49	44	81	7	20	30	64
47	57	10	5	42	76	71	27	34
24	31	68	63	16	53	39	73	2
79	8	45	28	65	21	13	50	60

[3] voir plus loin la définition de la multimagie

En effet, la somme des éléments sur chaque ligne, colonne, diagonale est égale à

$$\frac{9(9^2+1)}{2} = 369$$

et la somme des carrés des éléments sur chaque ligne, colonne et diagonale est égale à

$$\frac{9(2.9^2+1)(9^2+1)}{6} = 20049$$

1.1.7 bimagie partielle

Lorsque qu'un carré magique n'est pas bimagique, il peut être intéressant de compter sa *bimagie partielle*, c'est-à-dire le nombre de lignes ou colonnes ou diagonales dont les sommes sont égales à la constante de bimagie.

Si c est l'ordre du carré, il y a c lignes, c colonnes et 2 diagonales, et donc la bimagie partielle d'un carré est plus petite ou égale à $2c+2$ (égale lorsque le carré est bimagique). Nous parlerons de *composant* de bimagie partielle d'un carré magique pour désigner une ligne, colonne ou diagonale dont la somme est égale à la constante de bimagie.

Exemple d'un carré magique d'ordre 7, qui n'est pas bimagique mais qui possède 5 composants de bimagie : les lignes 3 et 4, les colonnes 5 et 6, ainsi que la contre-diagonale. En effet, la somme des carrés des éléments de ces composants est bien égale à la constante de bimagie (5775 pour l'ordre 7).

							5775
32	28	40	43	16	3	13	
10	48	25	5	29	21	37	
27	15	7	31	39	9	47	5775
19	38	8	23	6	46	35	5775
42	2	45	18	12	34	22	
44	33	20	14	24	36	4	
1	11	30	41	49	26	17	
				5775	5775		

1.1.8 Carré multimagique

En généralisant la définition de la bimagie, on définit la multimagie de la manière suivante :

Soit n un entier positif. Un carré est dit *n-multimagique* si, il est magique, et le reste lorsque l'on élève chacun des éléments aux différentes puissance $1, \ldots, n$.

Le nombre n est appelé le *degré de multimagie* du carré.

Remarques :

- on parle de carré *simplement magique* ou *de magie simple* lorsque le carré est 1-multimagique, c'est-à-dire magique mais pas bimagique.
- Un carré bimagique est donc un carré 2-multimagique.

1.2 Résultats connus pour la bimagie

Dans cette section, nous nous intéresserons aux résultats connus concernant la bimagie. Ce sont des résultats d'impossibilité de bimagie pour les ordres plus petits ou égaux à 7.

Sur le site de Lee Morgenstern[4] [Site Morgenstern] on trouve des preuves algébriques d'impossibilité pour les ordres 3, 4, 5 et 6. Sur ce même site, il est ébauché une preuve d'impossibilité pour l'ordre 7. Cependant, celle-ci n'est pas aboutie et ne peut donc être retenue.

Par contre, plusieurs auteurs, indépendamment, ont expérimentalement cherché des carrés bimagiques d'ordre 7 sans y parvenir. Ils ont utilisé, pour ce faire des logiciels différents, ce qui tend à montrer qu'il n'existerait aucun carré bimagique d'ordre 7.

1.2.1 Démonstrations algébriques

Nous allons montrer qu'il n'est pas possible de trouver des carrés bimagiques normaux pour les ordres 3, 4, 5 et 6. Pour les ordres 3 et 4,le résultat est plus général puisqu'il exprime l'impossibilité de trouver des carrés bimagiques pour des nombres entiers distincts.

Nous suivrons les démonstrations données par Lee Morgenstern su son site.

Ces démonstrations sont pour la plupart des manipulations algébriques. L'auteur introduit d'abord un petit lemme utile pour la suite.

Lemme de duplication

Soient a, b, c, d 4 entiers. Si :

$$a + b = c + d \text{ et} \tag{1.1}$$
$$a^2 + b^2 = c^2 + d^2 \tag{1.2}$$

alors $a = c$ ou $a = d$.

Démonstration :

Les équations 1.1et 1.2 peuvent être réécrites comme

$$a - c = d - b \text{ et} \tag{1.3}$$
$a^2 - c^2 = d^2 - b^2$ équivalent à
$$(a - c)(a + c) = (d + b)(d - b) \tag{1.4}$$

En utilisant 1.3, on remplace $(d - b)$ par $(a - c)$ dans 1.4 et on obtient :

$$(a - c)(a + c) = (a - c)(d + b) \equiv (a - c)[(a + c) - (d + b)] = 0 \text{ ou encore}$$
$$(a - c)[(a - d) + (c - b)] = 0 \tag{1.5}$$

Comme 1.1 est aussi équivalent à

$$a - d = c - b$$

[4]sur le site de C. Boyer [Site Multimagie] on apprend que L. Morgenstern est un mathématicien américain à la retraite.

l'équation 1.5 s'écrit :

$$(a-c)[(a-d)+(a-d)]=0 \tag{1.6}$$

et donc finalement $a=c$ ou $a=d$

CQFD

Ordre 3

Théorème : Il est impossible de trouver des carrés bimagiques d'ordre 3 composés de nombres entiers distincts.

Démonstration : la démonstration est purement algébrique et se fait par l'absurde : on commence par supposer que tous les nombres du carré sont distincts pour finalement arriver à une contradiction en utilisant le lemme de duplication.

Supposons qu'il existe un carré bimagique d'ordre 3 composé de nombres entiers distincts. Ecrivons le comme :

$$\begin{array}{ccc} a & b & P \\ Q & R & c \\ S & T & d \end{array}$$

où $a, b, c, d, P, Q, R, S, T$ sont des entiers quelconques mais distincts.

On a que $a+b+P=P+c+d$ puisque le carré est magique, c'est-à-dire :

$$a+b=c+d \tag{1.7}$$

De même, $a^2+b^2+P^2=P^2+c^2+d^2 \equiv$

$$a^2+b^2=c^2+d^2 \tag{1.8}$$

puisque le carré est bimagique. En appliquant le lemme de duplication aux équations 1.7 et 1.8, on obtient $a=c$ ou $a=d$ ce qui contredit le fait que tous les nombres du carré sont distincts.

CQFD

Ordre 4

Théorème : Il est impossible de trouver des carrés bimagiques d'ordre 4 composés de nombres entiers distincts.

Démonstration : même idée que précédemment. Supposons que

$$\begin{array}{cccc} a & M & N & b \\ P & Q & R & S \\ T & U & V & W \\ X & c & d & Y \end{array}$$

soit un carré bimagique d'ordre 4 (composés de nombres distincts).

Puisque que le carré est magique, on a

$$a+M+N+b=X+c+d+Y \tag{1.9}$$

$$a+Q+V+Y=M+Q+U+c \tag{1.10}$$

$$b+R+U+X=N+R+V+d \tag{1.11}$$

En additionnant ces trois équations, en éliminant les termes communs aux deux membres et en divisant par 2, on obtient finalement

$$a + b = c + d \tag{1.12}$$

En procédant aux mêmes calculs mais avec les carrés des éléments (puisque le carré est bimagique), on obtient également

$$a^2 + b^2 = c^2 + d^2 \tag{1.13}$$

Il suffit alors d'appliquer le lemme de duplication aux équations 1.12 et 1.13 pour obtenir $a = c$ ou $a = d$, donc une contradiction.

CQFD

Ordre 5

Théorème : il n'existe pas de carré bimagique *normal* d'ordre 5.

Démonstration : Nous avons développé la démonstration de Lee Morgenstern qui était trop succincte. La démonstration utilise l'arithmétique modulaire[5], et c'est ce qui fait son intérêt à nos yeux.

Les constantes de magie et de bimagie pour l'ordre 5 sont respectivement 65 et 1105.

Rappelons les résultats élémentaires de la théorie des nombres suivants :

- Tout nombre impair peut s'écrire comme $2x + 1$, x étant un entier quelconque.
- De la même manière, tout nombre pair peut s'écrire comme $2x$, x étant un entier quelconque.
- La somme de deux nombres pairs est un nombre pair.
- La somme de deux nombres impairs est un nombre pair.
- La somme d'un nombre pair et d'un nombre impair est un nombre impair.
- Le carré d'un nombre pair est un nombre pair.
- Le carré d'un nombre impair est un nombre impair.

1. Ecrivons 65 comme somme de 5 nombres :

   $$a + b + c + d + e = 65 \tag{1.14}$$

   Vu les rappels ci-dessus, il y a donc un nombre impair de nombres impairs dans cette somme.

   Par ailleurs, la somme bimagique, 1105, a pour reste 1 lorsqu'on la divise par 4 et par 8, ce qu'on écrit

   $$1105 \equiv 1 \ (mod\ 4) \tag{1.15}$$
   $$1105 \equiv 1 \ (mod\ 8) \tag{1.16}$$

[5] l'arithmétique modulaire sera définie rigoureusement dans le chapitre 2. Ici, on retiendra l'idée que $x\ mod(n)$ est égal au reste de la division entière de x par n.

Si la somme 1.14 est constitué de 5 nombres impairs, alors on a

$$65 = (2x_1 + 1) + (2x_2 + 1) + (2x_3 + 1) + (2x_4 + 1) + (2x_5 + 1)$$

Elevons chacun des termes au carré, on obtient

$$\begin{aligned} 1105 &= (2x_1 + 1)^2 + (2x_2 + 1)^2 + (2x_3 + 1)^2 + (2x_4 + 1)^2 + (2x_5 + 1)^2 \\ &= 4(x_1^2 + x_1 + x_2^2 + x_2 + x_3^2 + x_3 + x_4^2 + x_4 + x_5^2 + x_5) + 5 \end{aligned} \tag{1.17}$$

On se convainc que la somme dans la paranthèse donne un nombre pair : elle est formée de couple $x_i^2 + x_i$ qui par les propriétés rappelées plus haut ne peut être qu'un nombre pair.
L'équation 1.17 est donc de la forme

$$4(2X) + 5 = 8X + 5 \equiv 5 \ (mod\ 8) \tag{1.18}$$

et est donc différent de $1105 \equiv 1 \ (mod\ 8)$, ce qui est contradiction.

2. Si la somme 1.14 est constitué de 3 nombre impairs, alors on a

$$65 = (2x_1 + 1) + (2x_2 + 1) + (2x_3 + 1) + 2x_4 + 2x_5$$

A nouveau, en élevant les termes au carré, on obtient

$$\begin{aligned} 1105 &= (2x_1 + 1)^2 + (2x_2 + 1)^2 + (2x_3 + 1)^2 + (2x_4)^2 + (2x_5)^2 \\ &= 4(x_1^2 + x_1 + x_2^2 + x_2 + x_3^2 + x_3 + x_4^2 + x_4 + x_5^2 + x_5) + 3 \equiv 3 \ mod(4) \end{aligned} \tag{1.19}$$

Contradiction avec le fait que $1105 \equiv 1 \ (mod\ 4)$.

3. Reste la possibilité qu'il n'y ait qu'un seul nombre impair par ligne dans le carré. Mais alors, il y aurait $4 \times 5 = 20$ nombres pairs compris entre 1 et 25. Or il n'y en a que 12.

CQFD

Ordre 6

Théorème : il n'existe pas de carré bimagique normal d'ordre 6.

La démonstration utilise des techniques similaires à celles utilisées pour l'ordre 5 (arithmétique modulaire principalement). Cependant, les calculs sont plus longs et largement plus complexes. Dès lors, afin de ne pas alourdir le texte, nous renvoyons le lecteur intéressé sur le site de Lee Morgenstern [Site Morgenstern].

Ordre 7

Lee Morgenstern essaie d'appliquer les méthodes précédentes à l'ordre 7. Mais les arguments qu'il donne sont incomplets et donc non probants.

Nous n'avons pas trouvé d'autres essais de preuve pour les carrés normaux d'ordre 7. Christian Boyer, sur son site [Site Multimagie] évoque un mathématicien américain, D.N. Lehmer, qui, dans les années 30 se serait attaqué à la preuve de non existence pour l'ordre 7 ; mais il n'a, semble-t-il, pas atteint le résultat voulu.

Tournons-nous alors vers des méthodes expérimentales.

1.2.2 Résultats expérimentaux

Retour sur l'ordre 6

Nous avons vu plus haut qu'il n'existait pas de carrés bimagiques d'ordre 6. Cependant, en se restreignant à de la bimagique partielle, il existe des résultats intéressants.

Le Docteur A. Jacques nous a aimablement fourni les trois carrés suivants, fruits de ses recherches. Ils sont hémi-bimagiques, c'est-à-dire qu'ils sont magiques et, par ailleurs, bimagiques sur les lignes et les deux diagonales.

1	31	29	12	15	23
34	18	10	26	21	2
9	33	32	7	13	17
28	4	5	30	24	20
3	19	27	11	16	35
36	6	8	25	22	14

24	26	10	18	1	32
2	28	12	14	33	22
31	29	20	7	21	3
6	8	17	30	16	34
35	9	25	23	4	15
13	11	27	19	36	5

12	31	35	9	11	13
17	29	15	1	33	16
30	18	10	5	14	34
7	19	27	32	23	3
20	8	22	36	4	21
25	6	2	28	26	24

D'une communication personnelle[6] avec le Docteur Jacques, nous avons appris qu'il était supposé ne pas exister de tels carrés hémi-bimagiques.

Ordre 7

Sur son site, Christian Boyer expose des résultats expérimentaux pour l'ordre 7.

Partant de séries de lignes de 7 nombres compris entre 1 et 49 telles que :

- la somme des éléments de ces lignes fassent la constante de magie simple, 175.
- la somme des carrés des éléments de ces lignes fassent la constante de bimagie, 5 775.

Achille Rilly, en 1909, avait comptabilisé 1 844 lignes ayant les propriétés ci-dessus.

C. Boyer fait le raisonnement suivant :

1. La constante de bimagie de l'ordre 7, 5775 est de la forme $4k + 3$ avec k entier.
2. Le carré d'un nombre impair est de la forme $4k+1$, tandis que le carré d'un nombre pair est de la forme $4k$.
3. Dès lors, une somme de carrés de 7 termes doit contenir 3 ou 7 nombres impairs pour être de la forme $4k+3$.
4. Pour caser les 25 nombres impairs entre 1 et 49 sur des rangées de 7 éléments, la seule possibilité, pour répondre à la contrainte ci-dessus exprimée, est d'avoir 6 rangées avec 3 nombres impairs et 1 rangée avec 7 nombres impairs.
5. Parmi les 1844 lignes d'Achille Rilly, il en dénombre 60 qui sont composées de 7 nombres impairs.

[6] mai 2009

6. L'idée de sa méthode est d'alors choisir une de ces 60 lignes, puis compléter en puisant dans le "panier" des 1844 autres...

Quatre chercheurs, le français Christian Boyer, les allemands Walter Trump, Bogdan Golunski et le chinois Pan Fengchu, sont arrivés, de manière indépendante, au même résultat, à savoir que les meilleurs carrés magiques d'ordre 7 ont 13 composants de bimagique partielle.

Bien qu'aucune preuve de non existence formelle pour l'ordre 7 n'existe, on peut conclure provisoirement avec Walter Trump [Site Trump] : "I assume that there is no convincing mathematical reason for the nonexistence of these squares. It is just a matter of statistics. The probability for the existence of an order-7 bimagic square is very low."

Dans la suite de ce travail, nous allons aborder les carrés magiques suivant une voie différente, abstraite et nous aurons besoin de faire un détour dans le monde des structures algébriques.

Chapitre 2

Définition et explication des concepts mathématiques utilisés

Dans ce chapitre, nous allons présenter les outils mathématiques nécessaires à la compréhension de la méthode algébrique de génération de carrés multimagiques expliquée dans le chapitre suivant.

Il ne s'agit pas d'un manuel d'algèbre mais seules les notions utiles pour la suite seront introduites progressivement.

Dans ce chapitre, aucune démonstration ne sera présentée. En revanche, des exemples seront donnés pour éclairer les définitions et les notations.

Nous commencerons par rappeler quelques notions de base, ensuite celles de groupe, d'anneau, de matrice afin d'arriver à la notion de module qui est centrale dans le cadre de ce travail.

Pour l'écriture de ce chapitre, nous nous sommes basé principalement sur [Marco et *al* 2007 Vol1].

2.1 Notions préliminaires

2.1.1 Ensemble

Un ensemble E est une collection d'éléments, sans doublon et sans ordre.
Le nombre d'éléments de l'ensemble est appelé le cardinal et on le note $\#E$. Un ensemble est dit fini si son cardinal l'est, infini sinon.
Dans ce travail, on utilisera principalement des ensembles finis.

L'appartenance (non stricte) d'un sous-ensemble F de E sera noté $F \subseteq E$.
Soient E et F deux ensembles. Nous noterons $E \cap F$ leur intersection, $E \cup F$ leur union. Quant à l'ensemble vide, il sera noté ϕ

Le produit cartésien $E \times F$ est l'ensemble des couples (x_1, x_2) où $x_1 \in E$ *et* $x_2 \in F$.

2.1.2 Relation binaire

On appelle relation binaire sur un ensemble E toute partie du produit cartésien $E \times E$.
Pour toute relation R sur E et $\forall x, y \in E$, on note le fait que x est en relation avec y, xRy.

Exemple :

Soient $x, y, n \in \mathbb{N}, n > 0$.

En utilisant la division euclidienne par n, on a :
$x = q_1 * n + r_1$ *et* $y = q_2 * n + r_2$ pour $q_1, r_1, q_2, r_2 \in \mathbb{N}$, *et* $0 \leq r_1, r_2 < n$.

On définit la relation "avoir le même reste", notée mod_n par :

$x\ mod_n\ y\ ssi\ r_1 = r_2$.

Cette relation est également notée $x \equiv y\ (mod_n)$

2.1.3 Relation et classe d'équivalence

On appelle relation d'équivalence toute relation binaire R sur E qui est :

- réflexive : $\forall x \in E, xRx$.
- symétrique : $\forall x, y \in E, xRy\ ssi\ yRx$.
- transitive : $\forall x, y, z \in E, Si\ xRy\ et\ yRz\ alors\ xRz$.

Soit R une relation d'équivalence sur E. On appelle classe d'équivalence d'un élément x de E l'ensemble des $y \in E \mid xRy$. On la note $[x]$. N'importe quel élément d'une classe d'équivalence est un représentant de cette classe.

Exemple :

La relation mod_n définie ci-dessus est une relation d'équivalence. Les classes d'équivalence de cette relation sont $[0], [1], \ldots, [n-1]$ (les classes des différents restes possibles de la division par n).

2.1.4 Partition d'un ensemble - Ensemble quotient

Soit E un ensemble et R une relation d'équivalence.

On appelle partition de l'ensemble E tout famille $X = \bigcup F_i$ de sous-ensemble $F_i \neq \phi$ de E telle que :

1. $E = X$
2. $\forall F_i, F_j \in X : F_i \cap F_j = \phi$

Les classes d'équivalence d'une relation d'équivalence R sur E forment une partition de E (voir [Marco et *al* 2007 Vol1] Prop 7.82).

On appelle ensemble quotient et on note E/R l'ensemble des classes d'équivalence de R sur E.

Exemple :

L'ensemble quotient de $\mathbb{N}/mod_n$ est l'ensemble $\{[0], [1], \ldots, [n-1]\}$.

Il sera noté dans la suite $\mathbb{N}/n\mathbb{N}$.

2.1.5 Application

Une application f d'un ensemble A (appelé ensemble de départ) vers un ensemble B (appelé ensemble d'arrivée) est la donnée, pour tout élément de a de A, d'un et d'un seul élément b de B, appelé *image* de a :

$\forall a \in A, \exists!\ b \in B \mid b = f(a)$.

Pour tout élément y de B, on appelle *fibre* de y l'ensemble de ses antécédents (par f). On le note $f^{-1}(y)$.
$f^{-1}(y) = \{x \in A : f(x) = y\}$.

2.1.6 Application de $E \to E$

Cas particulier important : lorsque l'ensemble de départ est égal à l'ensemble d'arrivée.

L'application identité est définie comme : $Id_E : E \to E : Id_E(a) = a$.

Soit $f : E \to E$ une application de E dans lui-même.
On peut itérer l'application f comme suit :

$f^0 = Id_E$ et $f^n = f \circ f^{n-1}$, pour $n \geq 1$.

Dès lors, on définit *l'orbite* d'un élément a par rapport à f comme étant l'ensemble $\{f^k(a), k \geq 0\}$. On la note $O(a)$. Un élément a dont l'orbite est le singleton $\{a\}$ est appelé *point fixe*. Il possède la propriété que $f(a) = a$.

2.1.7 Injection - Surjection - Bijection

Soit $f : E \to F$ une application de E vers F. f est dite :

- *injective ssi* $\forall x, y \in E,\ f(x) = f(y) \Rightarrow x = y$. On dit que f est une injection. Cela traduit l'idée que 2 éléments différents dans l'ensemble de départ n'ont pas la même image.

- *surjective ssi* $\forall y \in F,\ \exists x \in E \mid y = f(x)$. On dit que f est une surjection. Cela traduit l'idée que tout élément de l'ensemble d'arrivée est l'image d'au moins un élément de l'ensemble de départ.

- *bijective ssi* f est injective et bijective. On dit que f est une bijection. Cela traduit l'idée qu'il y a une correspondance 1 à 1 entre les éléments des ensembles de départ et d'arrivée.

Les résultats suivants seront utilisés :

Si $\#E = \#F$, alors on a les équivalences suivantes :
f est injective *ssi* f est surjective *ssi* f est bijective (voir [Marco et *al* 2007 Vol1] Prop 8.12).

Inversément, si E et F sont finis, et si $f : E \to F$ est une bijection, alors $\#E = \#F$ (voir [Marco et *al* 2007 Vol1] Prop 8.7)

2.1.8 Arithmétique modulaire

Dans cette section, je vais définir les opérations d'addition et de multiplication pour l'ensemble quotient $\mathbb{N}/n\mathbb{N}$.

Soient $[x], [y]$ deux classes d'équivalence de l'ensemble quotient $\mathbb{N}/n\mathbb{N}$. On définit :

- addition modulo n : $[x] + [y] = [x + y]$. La somme de deux classe d'équivalence est la classe d'équivalence de la somme des deux représentants x, y de ces classes.

- produit modulo n : $[x] \times [y] = [x \times y]$. Le produit de deux classe d'équivalence est la classe d'équivalence du produit des deux représentants x, y de ces classes.

Ces opérations jouissent des propriétés suivantes :

- Elles sont bien définies car elles ne dépendent pas des représentants des classes.

- Elles sont associatives : $\forall [x], [y], [z] \in \mathbb{N}/n\mathbb{N}$:

  $([x] + [y]) + [z] = [x] + ([y] + [z])$
  et
  $([x] \times [y]) \times [z] = [x] \times ([y] \times [z])$.

- La loi $\times$ est distributive sur $+$: $\forall [x], [y], [z] \in \mathbb{N}/n\mathbb{N}$:

  $[x] \times ([y] + [z]) = [x] \times [y] + [x] \times [z]$
  et
  $([x] + [y]) \times [z] = [x] \times [z] + [y] \times [z]$.

Remarque :
Par extension, on utilisera l'arithmétique modulaire également sur les éléments $\{0, \ldots, n-1\}$ considérés comme *nombres* de $\mathbb{N}$ (et plus comme classes d'équivalence). Le calcul se faisant comme si ces nombres étaient les représentants des classes d'équivalence associées. Il y a une bijection entre l'ensemble $\mathbb{N}/n\mathbb{N}$ et l'ensemble $\{0, \ldots, n-1\}$

Exemple :
Si on calcule mod_5 :

$[2] + [4] = [1]$ car $2 + 4 = 6 \equiv 1(mod_5)$. Comme mentionnné, ces lois ne dépendent pas des représentants des classes : $17 \equiv 2(mod_5) \ + 29 \equiv 4(mod_5) = 46 \equiv 1(mod_5)$

$[2] \times [4] = [3]$ car $2 * 4 = 8 \equiv 3(mod_5)$

2.2 Monoïde

Un monoïde $(M, *)$ est un ensemble M doté d'une loi de composition interne $* : (M \times M) \rightarrow M$ qui :

- est associative : $\forall x, y, z \in M : (x * y) * z = x * (y * z)$
- possède un neutre : $\exists e \in M \mid \forall x \in M : e * x = x = x * e$

2.3 Groupe

Un groupe, noté en général $(G, *)$ est un monoïde dont tous les éléments sont inversibles :
$\forall x \in G : \exists x^{-1} \in G : x * x^{-1} = e_G = x^{-1} * x$ où e_G est le neutre du groupe.

Remarque :

L'inverse du produit $x * y$ est le "produit des inverses inversé" $y^{-1} * x^{-1}$. En effet :
$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * x^{-1} = e_G$.

Un groupe G est dit commutatif (ou abélien) si $\forall x, y \in G : x * y = y * x$

Remarque : lorsque la loi de composition est $+$, on parle d'opposé (et non d'inverse) d'un élément x et on le note $-x$.

Exemples :

1. $(\mathbb{Z},+)$: l'ensemble des entiers relatifs munis de l'addition habituelle est un groupe commutatif. Le neutre est évidemment le nombre 0.

2. $(\mathbb{N}/n\mathbb{N}, +)$: l'ensemble $\{[0], \ldots, [n-1]\}$ muni de l'addition modulo n est un groupe commutatif. Le neutre est $[0]$ et l'opposé d'un élément $[k]$ est l'élément $[n-k]$.

3. Soit p un nombre premier et soit l'ensemble $E = \{1, \ldots, p-1\}$.
   Si on munit E du produit modulo[1] p noté $\times$, $(E, \times)$ est un groupe commutatif. Le neutre est 1.
   En effet, *ssi* p est premier, on peut montrer (voir [Marco et *al* 2007 Vol1] chapitre 12-VI) que :
   - $\forall x, y \in \{1, \ldots, p-1\}, x \times y \neq 0$ (la loi $\times$ est interne).
   - $\forall k \in \{1, \ldots, p-1\} \exists\, k^{-1} \in \{1, \ldots, p-1\}$ tel que $k \times k^{-1} = 1$ (existence d'un inverse).
   - L'associativité decoule de celle de l'arithmétique modulaire (voir 2.1.8).

   La loi $\times$ peut être exprimée sous forme de table (appelée table de Cayley)[2].

[1] voir la remarque de 2.1.8

[2] dans la suite, ces tables seront utilisées pour exprimer les lois de composition, si une définition plus concise n'est pas disponible.

Voici un exemple pour l'ensemble $\{1, \ldots, 4\}$ et l'arithmétique modulo 5 :

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

On constate bien que la loi $\times$ est interne, que le neutre est 1 et que chaque élément dispose d'un inverse.

On identifiera ce groupe $(E, \times)$ avec l'ensemble $\mathbb{N}/p\mathbb{N} \setminus \{[0]\}$ muni de la multiplication de l'arithmétique modulaire.

4. Soit $(G, *)$ un groupe. On peut construire à partir de celui-ci un groupe à n dimensions : $(G^n, *)$ où chaque élément du groupe est un n-uplet $(g_1, \ldots, g_n)$ où la loi de composition agit composante par composante : $(g_1, \ldots, g_n) * (h_1, \ldots, h_n) = (g_1 * h_1, \ldots, g_n * h_n)$. Le neutre est le n-uplet $(e_G, \ldots, e_G)$ et l'inverse de $(g_1, \ldots, g_n)$ est $(g_1^{-1}, \ldots, g_n^{-1})$.

2.4 Sous-groupe

Un sous-groupe $(H, *)$ d'un groupe $(G, *)$ est un sous-ensemble H de G, qui muni de la même loi $*$ forme un groupe.

Etant donné un sous-groupe $(H, *)$ d'un groupe $(G, *)$, définissons une relation R sur G de la manière suivante : $\forall g_1, g_2 \in G : g_1 R g_2$ *ssi* $g_1^{-1} * g_2 \in H$. Deux éléments de G sont en relation si le produit de l'un par l'inverse de l'autre est dans H.

Cette relation est :

- réflexive : xRx puisque $x^{-1} * x = e_G \in H$ car H est un sous-groupe.
- symétrique : si xRy alors $x^{-1} * y \in H$ et comme H est un sous-groupe : $(x^{-1} * y)^{-1} = y^{-1} * x \in H$ et donc yRx.
- transitive : si xRy *et* yRz alors $x^{-1} * y \in H$ *et* $y^{-1} * z \in H \Rightarrow (x^{-1} * y) * (y^{-1} * z) = x^{-1} * z$ et donc xRz.

Il s'agit donc d'une relation d'équivalence et l'ensemble quotient G/R est noté G/H.

La classe d'équivalence d'un élément a est l'ensemble des éléments de type $\{a * h \mid h \in H\}$. En effet, $\forall h \in H$, $a^{-1} * ah = h \in H \Rightarrow aRah$ et par ailleurs, si $aRb \Rightarrow \exists h \in H \mid a^{-1} * b = h \Rightarrow b = ah$. Donc la classe d'équivalence est exactement $\{a * h \mid h \in H\}$.

Cet ensemble, noté aH, est appelé *classe à gauche de a modulo H*. Son cardinal est égal à celui de H.
Si la loi de groupe est $+$, cette classe est notée $a + H$.

Remarque :

Si G est abélien, on peut doter G/H d'une structure de groupe en posant $[x] * [y] = [x * y]$.
On parle alors de *groupe quotient.*

2.5 Homomorphisme

Un homomorphisme[3] est une application qui "conserve la structure". On parle d'homomorphisme de groupe, d'anneau, de corps, d'espace vectoriel, de module (voir plus loin).

Soient $(G_1, *_1), (G_2, *_2)$ deux groupes non nécessairement différents.

On appelle homomorphisme de groupe toute application $f : G_1 \to G_2$ tel que :

$f(x *_1 y) = f(x) *_2 f(y) \qquad x, y \in G_1$

Soit $f : G_1 \to G_2$ un homomorphisme. On appelle :

- Noyau, que l'on note $Ker(f)$ l'ensemble $\{x \in G_1 \mid f(x) = e_{G_2}\}$. C'est un sous-groupe de $(G_1, *_1)$.
- Image, que l'on note $Im(f)$ l'ensemble $\{f(x) \mid x \in G_1\}$. C'est un sous-groupe de $(G_2, *_2)$.

On appelle *isomorphisme* tout homomorphisme bijectif. Si il existe un isomorphisme entre $(G_1, *_1)$ et $(G_2, *_2)$, on dit que ces deux groupes sont *isomorphes*. Si $f : G \to G$ et f bijective, on dit que f est un automorphisme.

2.6 Anneau

Un anneau $(R, +, \times)$ est un ensemble R muni de deux lois $+$ et $\times$ telles que :

- $(R, +)$ est un groupe commutatif. Le neutre de cette loi est noté 0_R.
- $(R, \times)$ est un monoïde. Le neutre est noté 1_R et est $\neq 0_R$.
- la loi $\times$ est distributive sur la loi $+$:
  $\forall x, y, z \in R : x \times (y + z) = x \times y + x \times z$ *et* $(x + y) \times z = x \times z + y \times z$

Remarques :

- 0_R est absorbant pour la multiplication c'est-à-dire que :
  $\forall r \in R : r \times 0_R = 0_R \times r = 0_R$.
- Dans la littérature, on appelle (parfois) une telle structure, munie d'un neutre multiplicatif, un anneau unitaire. Par ailleurs, la condition $1_R \neq 0_R$ ne fait partie *stricto senso* de la définition d'un anneau ; mais comme dans ce travail on ne s'intéresse qu'aux anneaux unitaires, le seul anneau tel que $1_R = 0_R$ est celui réduit au seul élément $\{0_R\}$. En effet :
  Si $1_R = 0_R$, $\forall r \in R$, *on a* $: r = 1_R \times r = 0_R \times r = 0_R$.
- Un anneau est dit commutatif si la loi $\times$ est commutative : $\forall x, y \in A : x \times y = y \times x$.
- Un anneau est fini si le nombre d'éléments de R est fini (ce qui sera le cas des anneaux utilisés dans le cadre de ce mémoire). Le nombre d'éléments est appelé le *cardinal* de l'anneau.

[3] ou morphisme.

2.6.1 Unités d'un anneau

Un concept qui sera important par la suite est celui *d'unités d'un anneau.*

On notera $U(R)$ l'ensemble des éléments de l'anneau qui possèdent un inverse. Ces éléments seront appelés les *unités* de R.

Dans les exemples suivants, on décrira chaque fois l'ensemble $U(R)$.

Remarque : l'ensemble R privé de 0_R (c'est-à-dire $R \setminus \{0_R\}$) est noté R^*. En général, pour un anneau, cet ensemble est différent de $U(R)$.

2.6.2 Exemples d'anneaux :

1. $(\mathbb{Z}, +, \times)$ est l'anneau des entiers relatifs. Il est commutatif et les neutres de l'addition et de la multiplication sont respectivement 0 et 1.
   Dans cet anneau, les seuls éléments possédant un inverse sont 1 et -1. Dès lors $U(\mathbb{Z}, +, \times) = \{1, -1\}$.

2. $(\mathbb{N}/n\mathbb{N}, +, \times)$ est l'anneau de l'arithmétique modulo n $\forall n \in \mathbb{N}^*$. Il est commutatif et les neutres de l'addition et de la multiplication sont respectivement les classes [0] et [1].
   Les unités de cet anneau sont les classes dont les représentants sont premiers avec n.

3. Les exemples donnés jusqu'à présent pour les groupes et les anneaux faisaient intervenir des nombres et des opérations arithmétiques classiques ou modulaires .

   Les structures mathématiques de groupe et d'anneau sont beaucoup plus générales.
   Voici, un exemple emprunté à la théorie des fonctions :

   Soit $\mathbb{R}^{\mathbb{R}}$ l'espace des fonctions de $\mathbb{R} \to \mathbb{R}$. Pour toutes fonctions f, g de cet espace, on définit la somme et le produit de la façon suivante :
   $(f + g)(x) = f(x) + g(x)$ et $(f \times g)(x) = f(x)g(x)$.

   Muni de ces définitions, $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un anneau (voir [Marco et *al* 2007 Vol1] p.259).
   Pour cet exemple, le neutre pour la multiplication est la fonction constante $f_1(x) = 1$ $\forall x$ et l'ensemble des unités est constitué des fonctions f strictement non nulles (pour tout x), car alors on peut trouver, pour chacunes de celles-ci une fonction $g(x)$ telle que $f(x)g(x) = f_1(x) = 1$ $\forall x$.

4. Voici un anneau à 4 éléments : $\{0_R, 1_R, a, b\}$ avec les les lois $+$ et $\times$ suivantes :

$+$	0_R	1_R	a	b
0_R	0_R	1_R	a	b
1_R	1_R	0_R	b	a
a	a	b	0_R	1_R
b	b	a	1_R	0_R

$\times$	0_R	1_R	a	b
0_R	0_R	0_R	0_R	0_R
1_R	0_R	1_R	a	b
a	0_R	a	0_R	a
b	0_R	b	a	1_R

   Dans ce genre de construction, il s'agit de vérifier l'associativité et la distributivité de $\times$ sur $+$ (ce qui est bien le cas ici).
   Les unités de cet anneau sont les éléments 1 et b (remarquons la présence de 1_R dans la table $\times$ pour les entrées correspondantes).

5. Comme pour les groupes (voir Groupe ex 4), on construit des anneaux à n dimensions en partant d'un anneau R : l'anneau $(R^n, +, \times)$ abrégé dans la suite par R^n est l'anneau à n composantes, où les calculs se font composante par composante.
   Le neutre multiplicatif est le n-uplet $(1_R, \ldots, 1_R)$ et les unités sont les n-uplets dont chaque composante est une unité de l'anneau R.

2.7 Corps

Une structure particulière d'anneau que j'utiliserai est celle de corps.

Un corps est un anneau $(R, +, \times)$ tel que $(R^*, \times)$ est un groupe.[4]

Remarquons que pour un corps, $U(R) = R^*$ c'est-à-dire que tout élément du corps est unité sauf 0_R.

Exemples de corps :

1. $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ respectivement le corps des rationnels, le corps de réels et le corps des nombres complexes munis de l'addition et la multiplication habituelles sont des exemples bien connus de corps commutatifs.

2. $(\mathbb{N}/p\mathbb{N}, +, \times)$ où p est premier est un corps car on sait que c'est un anneau (voir Anneau exemple 2) et que $(\mathbb{N}/p\mathbb{N} \setminus \{[0]\}, \times)$ est un groupe (voir Groupe exemple 3). Ce corps sera utilisé par la suite.

3. Soit l'ensemble à 4 éléments $\{0_R, 1_R, a, b\}$ (voir Anneau exemple 4). En définissant une autre loi multiplicative, on en fait un corps :

$+$	0_R	1_R	a	b
0_R	0_R	1_R	a	b
1_R	1_R	0_R	b	a
a	a	b	0_R	1_R
b	b	a	1_R	0_R

$\times$	0_R	1_R	a	b
0_R	0_R	0_R	0_R	0_R
1_R	0_R	1_R	a	b
a	0_R	a	b	1_R
b	0_R	b	1_R	a

   En effet, on vérifie que pour chaque élément $k \in \{1_R, a, b\}$ $\exists k^{-1} \mid k \times k^{-1} = 1_R = k^{-1} \times k$.
   Ce corps est commutatif (car tout corps fini est commutatif - théorême de Wedderburn). Il sera également utilisé par la suite.

4. D'une manière générale, si p est un nombre premier, on montre que pour tout n, entier naturel positif, il existe un corps de cardinal p^n (voir [Marco et *al* 2007 Vol2] Chapitre 4 - section III) [5]. Pour $n = 1$, on retrouve l'exemple 2 ci-dessus.

2.8 Matrice

La notion de matrice est centrale dans la méthode présentée dans le chapitre suivant.
Une matrice est un tableau de n lignes et p colonnes d'éléments pris dans un anneau (ou un corps[6]) R. Chaque

[4] Pour certains auteurs ([Marco et *al* 2007 Vol1] par exemple), il faut également que l'anneau soit commutatif pour que ce soit un corps. La structure présentée ici est alors appelée *corps gauche*.

[5] sans entrer dans les détails de construction du corps, notons qu'il est lié à des quotients de polynômes. Les polynômes sont définis sur le corps $\mathbb{N}/p\mathbb{N}$.

[6] quand il s'agit d'un corps K, on obtient l'algèbre linéaire.

élément est indicé selon sa ligne et sa colonne : $a_{ij} \in R,\ 1 \leq i \leq n,\ 1 \leq j \leq p$.

Le couple (n, p) est appelé le format de la matrice.

On note (suivant [Monnier 2003]) :

- $M_{np}(R)$ l'ensemble des matrices de format (n, p) à éléments dans R.
- Une matrice $A \in M_{np}(R)$ est le tableau :

$$A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix}$$

Une *sous-matrice* d'une matrice A est une matrice pour laquelle on a sélectionné un sous-ensemble de lignes et de colonnes de la matrice A.

Une matrice de format $(n, 1)$ est appelée une *matrice colonne.*

2.8.1 Addition matricielle

L'addition de deux matrices $A, B \in M_{np}(R)$ définit une matrice $A + B$ de la manière suivante :

$(A + B)_{ij} = a_{ij} + b_{ij}$ (on somme les éléments correspondants) :

$$\begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1p} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{np} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1p} + b_{1p} \\ \vdots & & \vdots \\ a_{n1} + b_{n1} & \dots & a_{np} + b_{np} \end{pmatrix}$$

2.8.2 Produit matriciel

Le produit matriciel AB d'une matrice $A \in M_{np}(R)$ et d'une matrice $B \in M_{pq}(R)$ définit une matrice $C \in M_{nq}(R)$ telle que :

$C_{ij} = \sum_{k=1}^{p} a_{ik} \times b_{kj}$ (il s'agit du produit "ligne par colonne") :

$$\begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix} \times \begin{pmatrix} b_{11} & \dots & b_{1q} \\ \vdots & & \vdots \\ b_{p1} & \dots & b_{pq} \end{pmatrix} = \begin{pmatrix} c_{11} = \sum_{k=1}^{p} a_{1k} \times b_{k1} & \dots & c_{1q} = \sum_{k=1}^{p} a_{1k} \times b_{kq} \\ \vdots & & \vdots \\ c_{n1} = \sum_{k=1}^{p} a_{nk} \times b_{k1} & \dots & c_{nq} = \sum_{k=1}^{p} a_{nk} \times b_{kq} \end{pmatrix}$$

Propriétés du produit matriciel :

- Il est associatif.
- Il n'est pas commutatif.

2.8.3 Juxtaposition de matrices

Dans le cadre de ce travail, on utilisera la notation suivante :

Soient deux matrices A, B de format respectifs $(n, p_1), (n, p_2)$.

On forme la matrice M de format $(n, p_1 + p_2)$ juxtaposée de A *et* B que l'on note $M = (A\ B)$ dont les éléments sont

$$M = \begin{pmatrix} a_{11} & \dots & a_{1p_1} & b_{11} & \dots & b_{1p_2} \\ \vdots & & \vdots & & & \vdots \\ a_{n1} & \dots & a_{np_1} & b_{n1} & \dots & b_{np_2} \end{pmatrix}$$

On se servira de la juxtaposition "en colonnes" également :

Si A, B sont de format respectifs (n_1, p) et (n_2, p), on note $M = \begin{pmatrix} A \\ B \end{pmatrix}$ la matrice de format $(n_1 + n_2, p)$ définie par :

$$M = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n_1 1} & \dots & a_{n_1 p} \\ b_{11} & \dots & b_{1p} \\ \vdots & & \vdots \\ b_{n_2 1} & \dots & b_{n_2 p} \end{pmatrix}$$

2.8.4 Matrices carrées

Une classe importante de matrices est celle des matrices carrées $M_{nn}(R)$ $(n \geq 1)$ qui sera utilisé dans la suite. Nous dirons que la matrice de format (n, n) est d' *ordre n*.

$M_{nn}(R)$ dotée de l'addition et le produit matriciel forme un anneau non commutatif dont le neutre pour l'addition est la matrice nulle 0_n :

$$0_n = \begin{pmatrix} 0_R & \dots & 0_R \\ \vdots & & \vdots \\ 0_R & \dots & 0_R \end{pmatrix}$$

et celui de la multiplication est la matrice diagonale[7] $\mathbb{I}_n$

$$\mathbb{I}_n = \begin{pmatrix} 1_R & \dots & 0_R \\ \vdots & \ddots & \vdots \\ 0_R & \dots & 1_R \end{pmatrix}$$

Une matrice carrée A est dite inversible si il existe une matrice B telle que $A \times B = B \times A = \mathbb{I}_n$

L'ensemble des matrices carrées inversibles d'ordre n est noté $Gl_n(R)$.

[7] une matrice diagonale est une matrice carrée pour laquelle les seuls éléments (éventuellement) non nuls se trouvent sur la diagonale (les éléments de la forme a_{ii}).

Remarque :

Les carrés magiques d'ordre n sont évidemment des matrices carrées de type $M_{nn}(\mathbb{N})$. C'est d'ailleurs de cette manière qu'ils seront construits au chapitre suivant !

2.9 Déterminant

Pour ce travail, on aura besoin de savoir si un déterminant est nul ou pas. On se contentera de définir une méthode pour le calculer.

Le déterminant est une application $det : M_{nn}(R) \rightarrow R$ qui, à une matrice carrée d'ordre n fait correspondre un élément de R.

Pour calculer le déterminant d'une matrice, on choisit une ligne[8] i de la matrice et on calcule la somme :

$$det(A) = \sum_{j=1}^{n} sg(a_{ij}) \times (det(A_{\overline{ij}})) \qquad \text{où}$$

- $A_{\overline{ij}}$ est la sous-matrice de A pour laquelle on a retiré la ligne i et la colonne j
- $sg(a_{ij}) = (-1)^{i+j} a_{ij}$. Cette fonction alterne le signe de chaque élément de la matrice.
  Exemples : $sg(a_{11}) = a_{11}$ *car* $(-1)^{1+1} = 1$, $sg(a_{23}) = -a_{23}$ *car* $(-1)^{2+3} = -1$, *etc.*
- Le déterminant d'une matrice à un seul élément est l'élément lui-même.

Le calcul se fait donc récursivement en calculant des déterminants de sous-matrices pour arriver à une sous-matrice à un élément (qui est son propre déterminant).

Le déterminant d'une sous-matrice d'ordre k de la matrice A est appelé un *mineur d'ordre k* de A.

Donnons quelques exemples de calcul de déterminant (on calcule chaque fois par rapport à la première ligne) :

1. Une matrice de format $(2, 2)$

$$det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \times det(d) - b \times det(c) = a \times d - b \times c$$

2. Pour une matrice $A \in M_{nn}(R)$

$$det \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} = a_{11} \times det \begin{pmatrix} a_{22} & \dots & a_{2n} \\ \vdots & & \vdots \\ a_{n2} & \dots & a_{nn} \end{pmatrix} - a_{12} \times det \begin{pmatrix} a_{21} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

$$+ \quad \dots + (-1)^{1+n} a_{1n} \times det \begin{pmatrix} a_{21} & \dots & a_{2n-1} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn-1} \end{pmatrix}$$

[8] le calcul peut se faire également en travaillant sur une colonne.

3. Le déterminant de la matrice unité $\mathbb{I}_n$ est égal à 1_R.

Une propriété importante de la théorie des déterminants est que le déterminant d'un produit (de matrices) est égal au produit des déterminants :

$$det(AB) = det(A)det(B) \qquad \text{où } A, B \in M_{nn}(R)$$

Dès lors, pour qu'une matrice soit inversible, il faut que son déterminant soit une unité de l'anneau R. En effet :

$$det(A)det(A^{-1}) = det(AA^{-1}) = det(\mathbb{I}_n) = 1_R \Rightarrow det(A^{-1}) = (det(A))^{-1}$$

La réciproque est également vraie, à savoir que si le déterminant d'une matrice est une unité de R, alors elle est inversible. Nous utiliserons ce résultat dans la suite.

2.10 Module

Cette section se base sur sur les définitions de [Jeanneret 2008] Ch 14.

Un module[9] est la généralisation de la notion d'espace vectoriel lorsque l'on travaille avec un anneau au lieu d'un corps.

Plus formellement :

Soient $(R, +, \times)$ un anneau commutatif[10], $(M, +)$ un groupe abélien dont les éléments seront notés dans ce cadre $\overrightarrow{v}, \overrightarrow{v_1}, \overrightarrow{v_2}, \ldots$ et $'.'$ une application $R \times M \rightarrow M : r.\overrightarrow{v} \in M \ \forall r \in R \ et \ \forall \overrightarrow{v} \in M$ appelée multiplication scalaire que l'on notera, suivant en cela la tradition, plus simplement $r\overrightarrow{v}$

Un module M sur R est un triplet $(R, M, .)$ où R est un anneau, M un groupe abélien et . la multiplication scalaire définie ci-dessus telle que les propriétés suivantes soient respectées :

$\forall x, y \in R, \ \forall \overrightarrow{v}, \overrightarrow{v_1}, \overrightarrow{v_2} \in M$

- $x(\overrightarrow{v_1} + \overrightarrow{v_2}) = x\overrightarrow{v_1} + x\overrightarrow{v_2}$
- $(x + y)\overrightarrow{v} = x\overrightarrow{v} + y\overrightarrow{v}$
- $(x \times y)\overrightarrow{v} = x(y\overrightarrow{v})$
- $1_R\overrightarrow{v} = \overrightarrow{v}$

Remarques et exemples :

1. On dit que M est un R-module ou un module sur R.

2. Par analogie avec les espaces vectoriels, on appelera *vecteur* un élément du groupe d'un module et *scalaire* un élément de R. Ceci explique la notation "fléchée" pour les éléments du groupe.

[9] à ne pas confondre avec la notion d'arithmétique modulaire.

[10] on peut définir des modules à partir d'anneaux non commutatifs. On parle alors de module gauche. Dans ce travail, on utilisera des anneaux commutatifs.

3. Comme indiqué ci-dessus, lorsque $(R, +, \times)$ est un corps, on retrouve la notion d'espace vectoriel.

4. L'anneau R peut-être vu comme un module sur lui-même. En effet, la distributivité, l'associativité et l'existence d'un neutre pour la loi $\times$ correspond exactement aux propriétés ci-dessus. On parlera alors du module R.

5. A partir d'un anneau R^n (voir Anneau ex 5), on considèrera, comme dans l'exemple précédent, le module R^n sur R, que l'on notera également R^n. Pour cela, on posera : $\forall r \in R, \forall (x_1, \ldots, x_n) \in R^n$: $r(x_1, \ldots, x_n) = (r \times x_1, \ldots, r \times x_n)$ (on multiplie chaque composante par l'élément r).

6. On sait que $\mathbb{Z}$ est un anneau (voir Anneau ex 1). A partir du groupe $(\mathbb{N}/n\mathbb{N}, +)$ (voir Groupe ex 2), on crée le module $(\mathbb{N}/n\mathbb{N}, +)$ sur $\mathbb{Z}$: la multiplication est définie comme suit :
$\forall [x] \in \mathbb{N}/n\mathbb{N}$, $\forall z \in \mathbb{Z} : z[x] = [zx]$ (on multiplie le représentant x par z et on prend la classe d'équivalence).
Attention : il ne faut pas confondre ce module avec le module $(\mathbb{N}/n\mathbb{N}, +, \times)$ (comme dans l'exemple 4 ci-dessus) : dans ce dernier cas, les éléments que l'on multiplie sont eux-mêmes des classes d'équivalence tandis que dans le premier cas, il s'agit d'éléments de $\mathbb{Z}$. On verra que cela fait une différence : l'un est un module libre et l'autre pas (voir ci-dessous) !

2.11 Sous-module - module quotient

Un sous-module N d'un R-module M est un sous-groupe $(N, +)$ de $(M, +)$ telle que $\forall r \in R$ *et* $\forall \overrightarrow{v} \in N$: $r\overrightarrow{v} \in N$.

Soient M un R-module et N un sous-module de M. On peut munir le groupe quotient M/N d'une structure de R-module en posant $r[\overrightarrow{v}] = [r\overrightarrow{v}]$. On parle alors de *module quotient.*

2.12 Module libre

Les modules libres sont les modules qui ressemblent le plus aux espaces vectoriels. En effet, dans le cas général, il n'y a pas de notion de 'base' pour un module. Mais c'est le cas pour les modules libres.
Un R-module M est libre ssi il possède une base.

Les exemples les plus simples de module libre sont ceux définis dans les exemples 4 et 5 ci-dessus. C'est d'ailleurs avec ce dernier module que nous travaillerons exclusivement au chapitre suivant.

Rappel sur la notion de base (d'un module)[11] :

Une base d'un R-module M est un ensemble de n vecteurs $\overrightarrow{e_i}$ de M tels que :

1. Cet ensemble est une *partie génératrice* : tout vecteur de M est une combinaison linéaire des vecteurs de l'ensemble ; c'est-à-dire que tout vecteur $v \in M$ peut s'écrire :

$$\overrightarrow{v} = \sum_{i=1}^{n} \lambda_i \overrightarrow{e_i} \text{ où } \lambda_i \in R$$

[11] la notion de base est centrale en algèbre linéaire.

2. Cet ensemble est une *partie libre* c'est-à-dire que la combinaison linéaire ci-dessus est unique. Cette dernière condition est, en fait, équivalente à la condition suivante :

$$\sum \lambda_i \overrightarrow{e_i} = 0 \Rightarrow \lambda_i = 0, \forall i \in \{1, \ldots, n\}$$

C'est la condition 2 qui n'est pas respectée pour l'exemple 6 ci-dessus : $\forall n$, le module $(\mathbb{N}/n\mathbb{N}, +)$ sur $\mathbb{Z}$ ne possède aucune base car $n[x] = 0\ \forall [x] \in \mathbb{N}/n\mathbb{N}$. C'est la différence avec le module $(\mathbb{N}/n\mathbb{N}, +, \times)$ où on ne peut multiplier par $[n]$ (puisque $[n]$ n'appartient pas $\mathbb{N}/n\mathbb{N}$).

La *dimension* d'un module libre est le nombre de vecteurs de base (ce nombre est indépendant de la base choisie[12]).

2.13 Homomorphisme de module

Soient M, N deux R-modules.

Une application $h : M \to N$ est un homomorphisme de R-module si, pour tous $\overrightarrow{v}, \overrightarrow{v_1}, \overrightarrow{v_2} \in M,\ r \in R$:

1. $h(\overrightarrow{v_1} + \overrightarrow{v_2}) = h(\overrightarrow{v_1}) + h(\overrightarrow{v_2})$ Il s'agit de la propriété de morphisme de groupe

2. $h(r\overrightarrow{v}) = rh(\overrightarrow{v})$ On peut multiplier par le scalaire r avant ou après avoir appliqué h.

On utilisera le résultat suivant (voir [Jeanneret 2008] Prop 14.1.13) :

Théorême sur les modules :

Soit $h : M \to N$ un homomorphisme de R-module. Alors le module quotient $M/Ker(h)$ est isomorphe à $Im(h)$.

2.14 Matrice et homomorphisme

Une matrice M_{np} sur un anneau R représente un homomorphisme[13] de $R^p \to R^n$. Lorsqu'on travaille avec des modules libres, les p colonnes de la matrice représentent les images des p vecteurs de la base de R^p exprimés dans la base de R^n.

Les matrices (inversibles) de Gl_n expriment des automorphismes de R^n.

Un vecteur de R^n peut être représenté par une matrice colonne.
Un homomorphisme $L : R^p \to R^n$ appliqué à un vecteur $\overrightarrow{v}$ est représenté matriciellement par :

$$L(\overrightarrow{v}) = \begin{pmatrix} l_{11} & \ldots & l_{1p} \\ \vdots & \ldots & \vdots \\ l_{n1} & \ldots & l_{np} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_p \end{pmatrix}$$

[12] lorsque un module libre est défini à partir d'un anneau non commutatif, cette propriété n'est pas vraie. On ne peut donc parler de dimension dans ce cas.

[13] Lorsque R est un corps, on parle d'application linéaire entre espaces vectoriels.

Chapitre 3

Analyse de l'article de H. Derksen, C. Eggermont et A. van den Essen

Ce chapitre a pour but d'expliquer les résultats trouvés par Mrs Harm Derksen, Christian Eggermont, Arno van den Essen (voir [Multimagic Squares 2005]). Il s'agit d'une méthode algébrique de construction de carrés n-multimagiques (n étant le degré de multimagie).

Leur méthode est générale, en ce sens qu'ils prouvent que pour tout n donné, il est possible de trouver des carrés n-multimagiques. L'ordre de ces carrés devient, cependant, très grand quand n augmente.
Dans ce travail, comme on se limite à des petits ordres de carré, on l'utilisera pour produire des carrés simplement magiques et bi-magiques.

Etant donné la difficulté et la densité de cet article, j'expliquerai les définitions introduites, les lemmes et théorèmes à l'aide d'exemples. Les démonstrations données suivront celles de l'article mais seront beaucoup plus détaillées.

Les noms et numéros des lemmes et théorèmes seront ceux de l'article original.

Le cheminement se fera de la manière suivante :

Nous introduirons une certaine forme de bijection dont le Lemme 1.2 nous garantira l'existence. Le Lemme 1.3 nous fournira un résultat qui sera utile pour traiter le cas particulier de la multimagie de la contre-diagonale.

Le Lemme 1.4 est une transposition pour les modules d'un théorème connu de l'algèbre linéaire. Il énonce un résultat concernant le cardinal des fibres d'une application surjective de modules.

Ce résultat sera utilisé pour démontrer la Proposition 1.5, laquelle démontre que certaines sommes spécifiques qui font intervenir une application de modules surjective et des bijections, ne dépendent ni de l'application ni des bijections.

Cette proposition sera déterminante dans la démonstration de la constance des sommes des lignes, colonnes et diagonales des carrés construits à l'aide du théorème 2.2.

Ce théorème permet de construire des carrés n-multimagiques à condition que l'ordre de ces carrés soient q^n où q est le cardinal d'un anneau quelconque, R. Donc ces carrés auront q^n lignes, q^n colonnes et bien sûr q^{2n} éléments.

En faisant varier indépendemment 2 vecteurs a et b de R^n, on parcourra à l'aide de bijections de R^n vers $\{1, \ldots, q^n\}$ l'ensemble des indices des lignes (via a) et des colonnes (via b) du carré magique.

Pour la construction de ces carrés, nous aurons besoin de certaines matrices dites génératrices. Ces matrices définissent des automorphismes du module R^{2n} qui, s'appliquant à la juxtaposition de ces mêmes vecteurs a et b, balaieront l'ensemble des éléments du module R^{2n}. A nouveau, une bijection de R^{2n}, cette fois vers $\{1, \ldots, q^{2n}\}$ définira les *valeurs* des éléments du carré dans l'ensemble voulu.

Par ailleurs ces matrices génératrices seront construites de façon telle que la Proposition 1.5 pourra s'appliquer à certaines de leurs sous-matrices, ce qui garantira le caractère multimagique des carrés générés.

Voyons cela en détail.

3.1 Préliminaires

Dans la suite de ce chapitre, on utilisera un anneau fini R qui possède q éléments.
Si n est le degré de multimagie la méthode permet de générer des carrés d'ordre q^n.

On rappelle que $U(R)$ désigne l'ensemble des éléments inversibles (c'est à dire les unités) de l'anneau.

Par facilité, on notera ab le produit $a \times b$ de deux éléments $a, b \in R$.

Dans ce chapitre, les éléments du module R^n seront notés soit sous forme de vecteur, soit en les considérant comme des matrices colonnes.

On s'autorisera à ne pas toujours utiliser la notation 'fléchée' pour les vecteurs afin de ne pas alourdir le texte.

Le produit matriciel d'une matrice A et d'un vecteur u sera noté $A(u)$ ou même Au.

3.1.1 Définition 1.1 - Bijection de type c

Soit $E = \{0, \ldots, q-1\}$ le sous-ensemble à q éléments de $\mathbb{N}$.
Pour $c \in R$, on appelle bijection de type c, une bijection N de R vers E telle que :

$$N : R \to E \mid \ N(a) + N(-a + c) = q - 1$$

Remarque : le $+$ entre les deux termes $N(a)$ et $N(-a+c)$ est l'opération usuelle dans $\mathbb{N}$ tandis que les opérations intervenant dans le terme $N(-a + c)$ sont respectivement l'opposé et l'addition dans l'anneau R.

Exemples :

1. Soit $R = \mathbb{N}/5\mathbb{N}$ l'anneau (le corps) à 5 éléments dotés de l'arithmétique modulaire. La bijection $N : R \to E : [a] \to a$ qui, à une classe d'équivalence associe son représentant dans l'ensemble E, est de type [4]. En effet :

   $$N([0]) + N(-[0] + [4]) = 0 + N([0] + [4]) = 0 + N([4]) = 0 + 4 = 4$$

$N([1]) + N(-[1] + [4]) = 1 + N([4] + [4]) = 1 + N([3]) = 1 + 3 = 4$
$N([2]) + N(-[2] + [4]) = 2 + N([3] + [4]) = 2 + N([2]) = 2 + 2 = 4$
$N([3]) + N(-[3] + [4]) = 3 + N([2] + [4]) = 3 + N([1]) = 3 + 1 = 4$
$N([4]) + N(-[4] + [4]) = 4 + N([0]) = 4 + 0 = 4$

2. Avec le même anneau R et le même sous-ensemble E, on peut définir d'autres bijections :

   Soit $N : R \to E : [0] \to 1,\ [1] \to 2,\ [2] \to 3,\ [3] \to 4,\ [4] \to 0$ la bijection où on "ajoute 1 circulairement". Elle est de type [2]. En effet :

   $N([0]) + N(-[0] + [2]) = 1 + N([0] + [2]) = 1 + 3 = 4$
   $N([1]) + N(-[1] + [2]) = 2 + N([4] + [2]) = 2 + N([1]) = 2 + 2 = 4$
   $N([2]) + N(-[2] + [2]) = 3 + N([0]) = 3 + 1 = 4$
   $N([3]) + N(-[3] + [2]) = 4 + N([2] + [2]) = 4 + N([0]) = 4 + 0 = 4$
   $N([4]) + N(-[4] + [2]) = 0 + N([1] + [2]) = 0 + N([3]) = 0 + 4 = 4$

3. Soient $E = \{0, \ldots, 3\}$ et R l'anneau défini en 2.6 4 dont la table d'addition est :

$+$	0_R	1_R	a	b
0_R	0_R	1_R	a	b
1_R	1_R	0_R	b	a
a	a	b	0_R	1_R
b	b	a	1_R	0_R

   La bijection $N : R \to E : 0_R \to 2,\ 1_R \to 1,\ a \to 0,\ b \to 3$ est de type 1_R.
   En effet :

   $N(0_R) + N(-0_R + 1_R) = 2 + N(0_R + 1_R) = 2 + 1 = 3$
   $N(1_R) + N(-1_R + 1_R) = 1 + N(0_R) = 1 + 2 = 3$
   $N(a) + N(-a + 1_R) = 0 + N(a + 1_R) = 0 + N(b) = 0 + 3 = 3$
   $N(b) + N(-b + 1_R) = 3 + N(b + 1_R) = 3 + N(a) = 3 + 0 = 3$

3.1.2 Lemme 1.2

i. Si l'élément $(1_R + 1_R) \in U(R)$, alors il existe (au moins une) bijection de type c pour tout $c \in R$.
ii. Si l'élément $(1_R + 1_R)$ n'est pas dans $U(R)$, alors il existe (au moins une) une bijection de type c pour tout $c \in U(R)$.

Démonstration :

Définissons :

- $2_R = 1_R + 1_R$. Cette définition semble curieuse, mais méfions-nous : dans l'exemple 4 de Anneau (voir 2.6), on voit que $1_R + 1_R = 0_R$. Tout dépend donc de l'anneau !

- L'application, pour $c \in R,\ \varphi_c : R \to R : \varphi_c(a) = -a + c,\ \forall a \in R$.

On a $\varphi_c(\varphi_c(a)) = \varphi_c(-a + c) = -(-a + c) + c = a$. Dès lors, l'orbite de φ_c contient 1 ou 2 éléments (rappel : si elle en contient 1, c'est un point fixe). On vérifie qu'un élément est un point fixe *ssi* $2_R a = c$.

i. Dans ce cas, 2_R est une unité de R. Donc φ_c possède 1 seul point fixe, à savoir : $a_0 = 2_R^{-1}c$. L'orbite $O(a_0)$ possède donc 1 élément, les autres $O(a_1), O(a_2), \ldots, O(a_s)$ en possédant 2.

Donc $q = 2s + 1$ (en effet, il y s orbites à 2 éléments + 1 orbite à 1 élément, celle de a_0), et donc $s = \frac{q-1}{2}$.

Posons $N : R \to E : N(a_0) = s,\ N(a_i) = i - 1,\ N(\varphi_c(a_i)) = q - 1 - N(a_i)(= q - i)$.

Alors $N(a) + N(-a + c) = N(a) + N(\varphi_c(a)) = q - 1\ \forall a \in R$.

En effet :

$N(a_0) + N(\varphi_c(a_0)) = N(a_0) + N(a_0) = s + s = \frac{q-1}{2} + \frac{q-1}{2} = q - 1$,

$N(a_i) + N(\varphi_c(a_i)) = i - 1 + q - i = q - 1,\ a_i \in \{a_1, \ldots, a_s\}$ et

$N(a_i) + N(\varphi_c(a_i)) = N(\varphi_c(a_{i'})) + N(a_{i'}) = q - i' + i' - 1 = q - 1,\ a_i \in \{\varphi_c(a_1), \ldots, \varphi_c(a_s)\},\ a_i = \varphi_c(a_{i'})$

ii. Considérons maintenant le cas où 2_R n'est pas une unité. Pour $c \in U(R)$, φ_c n'a pas de point fixe. En effet :
si $\varphi_c(a) = a$, $2_R a = c$ et puisque c est unité, on a $cc^{-1} = 2_R(ac^{-1}) = 1_R$ et 2_R est inversible, donc on a une contradiction.

Donc toutes les orbites $O(a_1), \ldots, O(a_s)$ possèdent 2 éléments et par suite $s = \frac{q}{2}$.

Posons $N : R \to E : N(a_i) = i - 1,\ N(\varphi_c(a_i)) = q - 1 - N(a_i)(= q - i)$.

Alors $N(a) + N(-a + c) = N(a) + N(\varphi_c(a)) = q - 1\ \forall a \in R$.
En effet :
Remarquons que $R = \bigcup_{i=1}^{s} O(a_i)$ et donc tout élément de R se trouve dans une des orbites à 2 éléments.

$N(a_i) + N(\varphi_c(a_i)) = i - 1 + q - i$ pour $a_i \in \{a_1, \ldots, a_s\}$ et

$N(a_i) + N(\varphi_c(a_i)) = N(\varphi_c(a_{i'})) + N(a_{i'}) = q - i' + i' - 1 = q - 1$ pour $a_i \in \{\varphi_c(a_1), \ldots, \varphi_c(a_s)\}$ avec $a_i = \varphi_c(a_{i'})$

CQFD

Remarques :

- Ce lemme donne une méthode constructive pour définir une bijection de type c. On l'utilisera systématiquement par la suite pour faire varier les paramètres de bijection du programme.

- Comme tout anneau possède au moins une unité, à savoir l'élément 1_R, on peut donc toujours construire, au minimum, une bijection de type 1_R.

3.1.3 Bijection N_m

Soit $m \in \mathbb{N}^*$. Pour chaque $1 \leq j \leq m$, on choisit une bijection $N_{(j)}$ de type c_j, $c_j \in R$. C'est possible via le lemme 3.1.2.

Définissons l'application N_m du module R^m vers le sous-ensemble $\{1, \ldots, q^m\}$ de $\mathbb{N}$ de la façon suivante :

$N_m : R^m \to \{1, \ldots, q^m\} : N_m(a_1, \ldots, a_m) = 1 + \sum_{j=1}^{m} q^{j-1} N_{(j)}(a_j)$

Nous allons montrer que N_m est une bijection.

Pour deux vecteurs différents $\overrightarrow{u}, \overrightarrow{v} \in R^m$ montrons tout d'abord que $N_m(\overrightarrow{u}) \neq N_n(\overrightarrow{v})$.

En effet, N_m représente la décomposition d'un nombre appartenant à l'ensemble $\{1, \ldots, q^m\}$ en base[1] q puisque chaque coefficient de la somme est compris entre 0 et $q-1$ (les $N_{(j)}$ sont des applications vers l'ensemble $\{0, \ldots, q-1\}$). Cette décomposition est unique (si on ne tient pas compte des termes nuls apparaissant dans la somme).

Par ailleurs, $\overrightarrow{u} \neq \overrightarrow{v}$ veut dire que pour au moins 1 indice $k, u_k \neq v_k$ et comme les $N_{(j)}$ sont des bijections, $N_{(k)}(u_k) \neq N_{(k)}(v_k)$. Dès lors, on vient de montrer que N_m est une injection.

Comme $\#R^m = \underbrace{q.q \ldots q}_{m fois} = q^m = \#\{1, \ldots, q^m\}$, on en déduit, via le théorême de 2.1.7, que N_m est une bijection.

Cette bijection N_m a donc pour image l'ensemble de nombres allant de 1 à q^m. Ces nombres seront ceux rempliront le carré magique et donc rendront celui-ci normal (au sens du chapitre 1).

3.1.4 Lemme 1.3

Soit $\overrightarrow{c} = (c_1, \ldots, c_m)$ le vecteur des c_j liés aux bijections $N_{(j)}$.

Lemme 1.3 : $N_m(-\overrightarrow{u}) + N_m(\overrightarrow{u} + \overrightarrow{c}) = q^m + 1, \ \forall \overrightarrow{u} \in R^m$.

Démonstration :

$N_m(-\overrightarrow{u}) + N_m(\overrightarrow{u} + \overrightarrow{c}) = 1 + \sum_{j=1}^{m} q^{j-1} N_{(j)}(-u_j) + 1 + \sum_{j=1}^{m} q^{j-1} N_{(j)}(u_j + c_j)$

$= 2 + \sum_{j=1}^{m} q^{j-1}(N_{(j)}(-u_j) + N_{(j)}(u_j + c_j))$

$= 2 + \sum_{j=1}^{m} q^{j-1}(q-1)$ (*puisque les* $N_{(j)}$ *sont de type* c_j)

$= 2 + (1 + q + \ldots + q^{m-1})(q-1) = 2 + (q^m - 1) = q^m + 1$

CQFD

Ce n'est que dans ce lemme que l'on utilise le fait que les bijections sont de type c.

Par ailleurs, ce lemme sera utile uniquement pour prouver la n-multimagie de la contre-diagonale dans la démonstration du théorème 2.2 ci-dessous.

[1] base s'entendant au sens arithmétique du terme, comme dans base binaire, base décimale, ...

3.1.5 Application affine

Une application affine (de modules) $L : R^n \to R^s$, $n, s \in \mathbb{N}^*, n \geq s$ est une application telle qu'il existe un homomorphisme de modules $L_0 : R^n \to R^s$ et un vecteur $v \in R^s$ telle que :

$L(a) = L_0(a) + v, \qquad a \in R^n$

Remarque :

Si L est surjective, alors L_0 l'est également. En effet :

Soit $y \in R^s$. Et soit $y_1 = y + v \in R^s$ $\exists a \in R^n : L(a) = y_1$ par la surjectivité de L.
On a $L(a) - v = L_0(a) = y + v - v = y$.
Et donc $\forall y \in R^s$, $\exists a \in R^n : L_0(a) = y$

3.1.6 Lemme 1.4

Lemme 1.4 : Si $L : R^n \to R^s$ est une application affine de modules surjective, alors

$\#L^{-1}(y) = q^{n-s}$, $\forall y \in R^s$ (le cardinal des fibres est constant)

Démonstration :

Soit $y \in R^s$. Puisque L est surjective, $\exists a_0 \mid L(a_0) = y$.

Montrons que[2] $L^{-1}(y) = a_0 + Ker(L_0)$. En effet :

i. Soit $x \in Ker(L_0)$. On a : $L(a_0 + x) = L_0(a_0 + x) + v$

$= L_0(a_0) + L_0(x) + v$ (L_0 est un homomorphisme)

$= L_0(a_0) + 0 + v$ (x est dans le noyau de L_0)

$= L_0(a_0) + v = L(a_0) = y$

On en déduit que $a_0 + x \in L^{-1}(y)$ et donc $a_0 + Ker(L_0) \subseteq L^{-1}(y)$

ii. Soit $x \in L^{-1}(y)$

Alors $L_0(x - a_0) = L_0(x) - L_0(a_0) = y - y = 0$

$\Rightarrow x - a_0 = x' \in Ker(L_0) \Rightarrow x = a_0 + x' \in a_0 + Ker(L_0)$

et donc $L^{-1}(y) \subseteq a_0 + Ker(L_0)$.

Donc $\#L^{-1}(y) = \#(a_0 + Ker(L_0)) = \#Ker(L_0)$ (voir 2.4).

Comme L_0 est surjective (voir remarque 3.1.5), $Im(L_0) = R^s$. Par le théorême sur les modules (voir 2.13),

[2] $a_0 + Ker(L_0)$ est la classe à gauche de a_0 modulo $Ker(L_0)$ (voir 2.4).

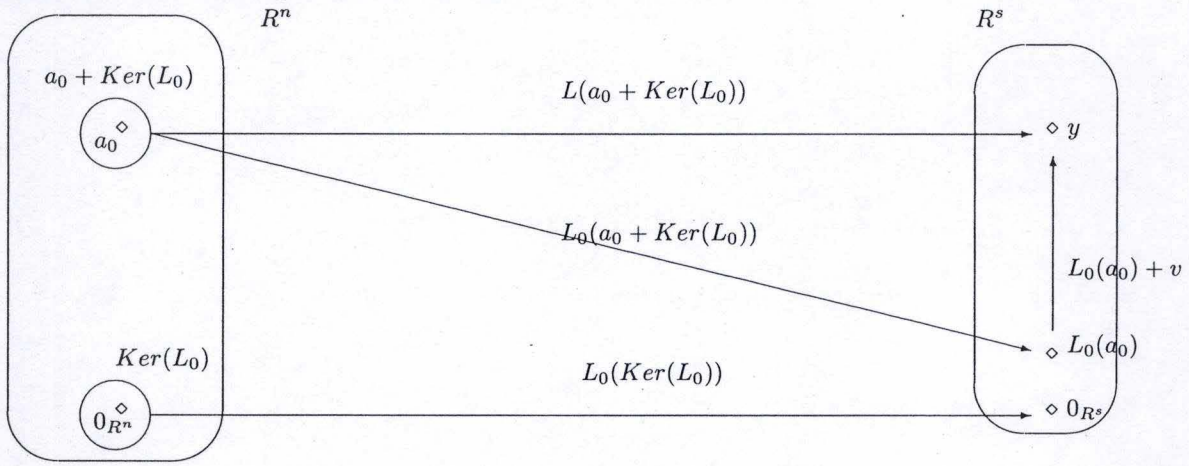
$R^n/Ker(L_0)$ est isomorphe à R^s et comme $\#R^n = q^n$ et que $\#R^s = q^s$ il s'ensuit que $\#Ker(L_0) = q^{n-s}$

$CQFD$

Remarque :

Comme $L^{-1}(y) = a_0 + Ker(L_0)$, les fibres forment une partition de R^n.

On peut illustrer ce lemme par le dessin suivant :



3.1.7 Proposition 1.5

Soit $L : R^n \to R^s$ une application affine surjective. Pour chaque $j \in \{1, \ldots, s\}$ donnons-nous $N_{(j)}$ une bijection de $R \to E$. $\forall e_1, \ldots, e_s \in \mathbb{N}$ on a :

$$\sum_{a \in R^n} (N_1(L(a)_1))^{e_1} \ldots (N_s(L(a)_s))^{e_s} = q^{n-s}(\sum_{i=0}^{q-1} i^{e_1}) \ldots (\sum_{i=0}^{q-1} i^{e_s})$$

Remarques :

1. Cette proposition veut dire que l'on fait la somme sur tous les éléments de R^n du produit des composantes $L(a)_1, \ldots, L(a)_s$ de l'application L, 'bijectés" chacune sur $\{0, \ldots, q-1\}$ puis élevés à une certaine puissance (différentes pour chacune de composantes).
   La proposition énonce que cette somme ne dépend ni de L, ni d'aucune des bijections $N_{(j)}$.

2. Les bijections considérées ici sont quelconques (elle ne doivent pas être de type c).

Démonstration :

Soit $y = (y_1, \ldots, y_s) \in R^s$. Alors $\forall a \in L^{-1}(y)$ on a

$$(N_{(1)}(L(a)_1))^{e_1} \ldots (N_{(s)}(L(a)_s))^{e_s} = (N_{(1)}(y_1))^{e_1} \ldots (N_{(s)}(y_s))^{e_s}$$

La somme sur les éléments de la fibre donne :

$$\sum_{a \in L^{-1}(y)} (N_{(1)}(L(a)_1))^{e_1} \ldots (N_{(s)}(L(a)_s))^{e_s} = q^{n-s}(N_{(1)}(y_1))^{e_1} \ldots (N_{(s)}(y_s))^{e_s} \tag{3.1}$$

Tous les a de la fibre sont envoyés sur y par L et il y a q^{n-s} éléments dans la fibre (Lemme 1.4).

Comme les fibres forment une partition de R^n (voir remarque du Lemme précédent), et comme L est surjective, c'est-à-dire que tous les y de R^s apparaissent dans la somme, on peut regrouper les termes de celle-ci :

$$\sum_{a \in R^n} = \sum_{y \in R^s} \sum_{a \in L^{-1}(y)}$$

ce qui donne

$$\sum_{a \in R^n} (N_1(L(a)_1))^{e_1} \ldots (N_s(L(a)_s))^{e_s} = \sum_{y \in R^s} \sum_{a \in L^{-1}(y)} (N_1(L(a)_1))^{e_1} \ldots (N_s(L(a)_s))^{e_s}$$

En utilisant 3.1

$$= \sum_{y \in R^s} q^{n-s}(N_{(1)}(y_1))^{e_1} \ldots (N_{(s)}(y_s))^{e_s}$$

On ré-arrange les termes de la somme de la manière suivante :

Soient $y_1^{(1)}, \ldots, y_1^{(q)}$ les q valeurs particulières que prend y_1. La somme sur $y \in R^s$ s'écrit alors :

$$q^{n-s}(N_{(1)}(y_1^{(1)}))^{e_1}\Big(\sum_{y_2 \in R, \ldots, y_s \in R} (N_{(2)}(y_2))^{e_2} \ldots (N_{(s)}(y_s))^{e_s}\Big) +$$

$$\vdots$$

$$+$$

$$q^{n-s}(N_{(1)}(y_1^{(q)}))^{e_1}\Big(\sum_{y_2 \in R, \ldots, y_s \in R} (N_{(2)}(y_2))^{e_2} \ldots (N_{(s)}(y_s))^{e_s}\Big) = \text{(en factorisant)}$$

$$q^{n-s}\Big(\sum_{y_1 \in R} (N_{(1)}(y_1))^{e_1}\Big)\Big(\sum_{y_2 \in R, \ldots, y_s \in R} (N_{(2)}(y_2))^{e_2} \ldots (N_{(s)}(y_s))^{e_s}\Big)$$

En réitérant sur les variables $y_2, \ldots, y_s$ on obtient finalement :

$$= q^{n-s}\Big(\sum_{y_1 \in R} (N_{(1)}(y_1))^{e_1}\Big) \ldots \Big(\sum_{y_s \in R} (N_{(s)}(y_s))^{e_s}\Big)$$

Comme les $N_{(j)}$ sont des bijections, tous les éléments de $\{0, \ldots, q-1\}$ apparaîtront une et une seule fois dans chacune des sommes $(\sum_{y_j \in R}(N_{(j)}(y_j))^{e_j})$ et donc chacune de ces sommes sera égale à

$$\sum_{i=0}^{q-1} i^{e_j}$$

CQFD

3.2 Construction du carré n-multimagique

Dans cette section, nous dérivons le résultat central du mémoire. Pour commencer, fixons les notations.

Soit n le degré de multimagie.

Comme d'habitude, R est un anneau à q éléments.

3.2.1 Choix de bijections

Choisissons $c_1, \ldots, c_n$ dans R et n bijections de type $c_1, \ldots, c_n$

$$N_{(1)}, \ldots, N_{(n)} : R \to \{0, \ldots, q-1\}$$

Remarquons que ces bijections ne doivent pas être nécessairement différentes. Elles vont nous permettre de définir une autre bijection :

$$N_n : R^n \to \{1, \ldots, q^n\}$$

comme décrit en 3.1.3.

De la même manière, choisissons $c'_1, \ldots, c'_{2n}$ et $2n$ bijections de type $c'_1, \ldots, c'_{2n}$

$$N'_{(1)}, \ldots, N'_{(2n)} : R \to \{0, \ldots, q-1\}1$$

Avec ces bijections, on s'en donne une autre (voir 3.1.3) :

$$N'_{2n} : R^{2n} \to \{1, \ldots, q^{2n}\}$$

3.2.2 Définition 2.1 - Matrices génératrices

Une matrice $X \in Gl_{2n}(R)$ est dite *génératrice n-multimagique* si elle est la juxtaposée de deux matrices $A, B \in M_{2n,n}$ (c'est-à-dire $X = (A\ B)$) qui sont telles que tous les mineurs d'ordre n de $A, B, A+B, A-B$ sont des unités de R.

L'ordre d'une matrice génératrice est donc liée au degré de multimagie. Pour la simple magie, la matrice génératrice est d'ordre 2 et pour la bimagie, d'ordre 4.

Exemples :

1. Dans cet exemple, on s'occupe de la simple magie, et on utilise comme anneau $R = \mathbb{N}/5\mathbb{N}$, le corps à 5 éléments avec l'arithmétique modulaire. On construit la matrice X génératrice 1-multimagique à partir des matrices A et B suivante :

$$A = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \qquad B = \begin{pmatrix} 3 \\ 4 \end{pmatrix} \qquad \text{et donc} \qquad X = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$$

   Comme il s'agit d'un corps, rappelons que les unités sont les éléments différents de 0.

   Le déterminant de X est égal à (tous les calculs se font modulo 5) :

$$det(X) = 1 \times 4 - 3 \times 2 = 4 - 1 = 3 \in U(R)$$

Les mineurs d'ordre $n(=1)$ de A sont 1 *et* $2 \in U(R)$.
Les mineurs d'ordre $n(=1)$ de B sont 3 *et* $4 \in U(R)$.
Les mineurs d'ordre $n(=1)$ de $A+B$ sont $1+3=4$ *et* $2+4=1 \in U(R)$.
Les mineurs d'ordre $n(=1)$ de $A-B$ sont $1-3=3$ *et* $2-4=3 \in U(R)$.

La matrice X vérifie les conditions et est donc une matrice génératrice.

2. Toujours pour la magie simple, mais avec le corps à 4 éléments décrit en 2.7 exemple 3, la matrice

$$X = \begin{pmatrix} 1 & a \\ 1 & b \end{pmatrix}$$

est génératrice. Tous les éléments de X (et donc tous les mineurs d'ordre 1 de A et B) sont des unités de R. Par ailleurs, $1+a=b, 1+b=a, 1-a=b, 1-b=a$ *et* $det(X)=b-a=1_R$ sont aussi tous des unités de R.

3. Avec le même corps, mais pour la bimagie ($n=2$), considérons la matrice suivante :

$$X = \begin{pmatrix} 1 & 0 & a & 1 \\ 0 & a & a & a \\ a & a & a & 0 \\ 1 & a & 0 & 1 \end{pmatrix}$$

On vérifie que les éléments suivants sont des unités de R :

- Le déterminant de X $(=a)$

- Tous les mineurs d'ordre n $(=2)$ de A, cad les déterminants des matrices :

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a & a \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & a \end{pmatrix}, \begin{pmatrix} 0 & a \\ a & a \end{pmatrix}, \begin{pmatrix} 0 & a \\ 1 & a \end{pmatrix}, \begin{pmatrix} a & a \\ 1 & a \end{pmatrix}$$

- Tous les mineurs d'ordre n $(=2)$ de B, cad les déterminants des matrices :

$$\begin{pmatrix} a & 1 \\ a & a \end{pmatrix}, \begin{pmatrix} a & 1 \\ a & 0 \end{pmatrix}, \begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & a \\ a & 0 \end{pmatrix}, \begin{pmatrix} a & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$$

- De même, tous les mineurs d'ordre 2 des matrices $A+B$ et $A-B$.

  Après tout ce travail, on est récompensé : X est génératrice 2-multimagique !

- Voici un exemple pour lequel il ne peut y avoir de matrice génératrice :
  Soit le corps à 2 éléments $\mathbb{N}/2\mathbb{N}$ (muni donc de l'arithmétique modulaire).

  Pour la magie simple, les mineurs doivent être unités. Or, le seul élément inversible étant 1, les 4 éléments de la matrice X devraient valoir 1, mais alors, entre autre, la somme des lignes est égale à 0 qui n'appartient pas à $U(R)$.

  Pour la bimagie, la matrice A sera de format $(4,2)$. Ses 4 lignes doivent être différentes 2 à 2 (sinon il existerait un mineur d'ordre 2 nul). Les seules variations possibles sont $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ et donc, tout mineur formé à partir de la ligne $(0,0)$ sera nul.

3.2.3 Théorème 2.2

Voici le théorème principal qui permet de construire des carrés n-multimagiques.

Théorème 2.2 : Soit $X \in Gl_{2n}(R)$ une matrice génératrice n-multimagique. Pour tout $t \in R^{2n}$,

la matrice M de format (q^n, q^n) définie par

$$M_{N_n(a),N_n(b)} = N'_{2n}\left(X \begin{pmatrix} a \\ b \end{pmatrix} + t\right), \qquad a, b \in R^n \tag{3.2}$$

est n-multimagique.

Remarques :

1. Comme expliqué en 2.8.3, $\begin{pmatrix} a \\ b \end{pmatrix}$ représente la juxtaposition des deux vecteurs a et b.
2. $X \begin{pmatrix} a \\ b \end{pmatrix}$ est le produit matriciel de la matrice X et de la juxtaposition ci-dessus.
3. La matrice M d'ordre q^n est bien définie, c'est-à-dire que le membre de droite dans la formule ci-dessus défini une valeur pour chaque élément de la matrice. En effet, les indices de ligne et de colonne sont donnés par la bijection N_n. Les valeurs d'indice parcourent bien l'ensemble $\{1, \ldots, q^n\}$ lorsque a et b varient dans R^n. Donc tous les éléments de la matrice M seront atteints une et une seule fois.
4. La matrice M comporte q^{2n} éléments. Puisque X est dans Gl_{2n}, X est inversible et donc définit un automorphisme de R^{2n} (voir 2.13). Dès lors tous les vecteurs de R^{2n} sont parcourus par cet automorphisme appliqué à $\begin{pmatrix} a \\ b \end{pmatrix}$, vecteur de R^{2n}, quand a et b varient dans R^n.

   Remarque : l'ajout du vecteur (constant) $t \in R^{2n}$ ne change rien à ce fait.
5. Puisque la bijection N'_{2n} est appliquée à tous les vecteurs de R^{2n}, tout l'ensemble $\{1, \ldots, q^{2n}\}$ sera atteint, et donc M est normale.

Reste donc à montrer que M est n-multimagique.

3.2.4 Démonstration du théorême 2.2

Formule du multinôme

La formule suivante sera utile pour la suite de la démonstration.

Formule du multinôme (tirée de [Marco et *al* 2007 Vol1] Prop. 8.41) :
Pour $x_1, \ldots, x_n, d \in \mathbb{N}$ (les x_i pourraient également être dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$)

$$(x_1 + \ldots + x_n)^d = \sum_{e_1+\ldots+e_n=d} \frac{d!}{e_1! \ldots e_n!} x_1^{e_1} \ldots x_n^{e_n} \text{ avec } e_1, \ldots, e_n \in \mathbb{N}$$

Dans la suite, nous aurons à calculer des sommes de type $(1 + x_1 + \ldots + x_n)^d$

$$(1 + x_1 + \ldots + x_n)^d = 1 + \sum_{\substack{e_1+\ldots+e_s \leq d \\ e_1,\ldots,e_s \geq 1}} \frac{d!}{e_1! \ldots e_s!} x_{j_1}^{e_1} \ldots x_{j_s}^{e_s} \tag{3.3}$$

où on ne considère qu'un sous-ensemble des variables x_i (le sous-ensemble $x_{j_1} \dots x_{j_s}$), chacune de ces variables à la puissance e_i strictement plus grand que 0. s est le nombre de variables x_i différentes intervenant dans chaque terme de la somme et s varie d'un terme à l'autre.

Remarquons que s est toujours plus petit ou égal à d.

Chaque terme est multiplié par une certaine constante $\frac{d!}{e_1!\dots e_s!}$.

Dans la suite, nous appelerons *somme multinomiale* la somme ci-dessus.

Pour la suite des explications, on appelera *signature* du terme le triplet constitué des valeurs de s, de $\frac{d!}{e_1!\dots e_s!}$, et de l'ensemble des couples formés par les variables x_{j_i} et leur exposant associé e_i pour $1 \leq i \leq s$.

Exemple :

$$(1 + x_1 + x_2)^2 = (1 + x_1 + x_2)(1 + x_1 + x_2) = 1 + 2x_1^1 + 2x_2^1 + x_1^2 + x_2^2 + 2x_1^1 x_2^1$$

Exemples de quelques signatures de cette somme multinomiale :

signature$(2x_1) = (1, 2, \{(x_1, 1)\})$, signature$(x_1^2) = (1, 1, \{(x_1, 2)\})$, signature$(2x_1x_2) = (2, 2, \{(x_1, 1), (x_2, 1)\})$, ...

On constate que la structure de la somme du membre de droite de (3.3) ne dépend que du nombre de termes (n) apparaissant dans le membre de gauche et de l'exposant d. Par structure, on entend le nombre de termes (du membre de droite) et la signature de ceux-ci. Cette structure ne dépend aucunement de la *valeur* des variables x_i.

Revenons à la matrice M. Le membre de droite de (3.2) est image de la bijection N'_{2n} et est donc par définition des N'_m (cf 3.1.3) de la forme $1 + \sum_{j=1}^{2n} q^{j-1} N'_{(j)}(v_j)$ où $v_j \in R$. En elevant ce terme à la puissance d, on obtient une somme multinomiale. Comme tous les éléments de la matrice M ont la même forme, leur somme multinomiale aura donc la même structure.

Somme sur les colonnes

Montrons que la somme des éléments, chacun élevé à la puissance d, de chaque colonne de la matrice M est une constante pour tout $1 \leq d \leq n$.

Fixons le vecteur b. En faisant varier le vecteur a dans R^n, on parcourt toute la colonne $N_n(b)$.

Définissons $S_b(d)$, la somme de chaque élément de la colonne $N_n(b)$ élevés à la puissance d :

$$S_b(d) = \sum_{a \in R^n} M^d_{N_n(a), N_n(b)}$$

Montrons que cette somme ne dépend pas de b (donc elle a la même valeur pour chaque colonne).

Détaillons le calcul :

1. La j^{eme} composante du vecteur $X \begin{pmatrix} a \\ b \end{pmatrix} = (A\ B) \begin{pmatrix} a \\ b \end{pmatrix}$ est égale à $A_{(j)}a + B_{(j)}b$ où $A_{(j)}$ (resp. $B_{(j)}$) est la j^{eme} ligne de la matrice A (resp. B). Il s'agit donc du produit matriciel de la j^{eme} ligne de A (resp. B) et de a (resp. b). Notons :

$$C_j(a, b) = q^{j-1} N'_{(j)}(A_{(j)}a + B_{(j)}b + t_j)\ \forall j \in \{1, \dots, 2n\}$$

2. $M^d_{N_n(a),N_n(b)} = \left(N'_{2n}\left(X\begin{pmatrix} a \\ b \end{pmatrix}+t\right)\right)^d = \left(1+\sum_{j=1}^{2n} C_j(a,b)\right)^d$ puisque N'_{2m} est défini comme en 3.1.3.

3. La somme $\left(1+\sum_{j=1}^{2n} C_j(a,b)\right)^d$ peut donc être écrite comme somme multinomiale

$$1+\sum_{\substack{e_1+\ldots+e_s\leq d\\ e_1,\ldots,e_s\geq 1}} \frac{d!}{e_1!\ldots e_s!} C_{j1}(a,b)^{e_1}\ldots C_{j_s}(a,b)^{e_s}$$

On obtient

$$\begin{aligned} S_b(d) &= \sum_{a\in R^n}\left(1+\sum_{\substack{e_1+\ldots+e_s\leq d\\ e_1,\ldots,e_s\geq 1}} \frac{d!}{e_1!\ldots e_s!} C_{j1}(a,b)^{e_1}\ldots C_{j_s}(a,b)^{e_s}\right) \\ &= q^n+\sum_{\substack{e_1+\ldots+e_s\leq d\\ e_1,\ldots,e_s\geq 1}} \frac{d!}{e_1!\ldots e_s!}\sum_{a\in R^n} C_{j1}(a,b)^{e_1}\ldots C_{j_s}(a,b)^{e_s} \quad \text{(en permutant les sommes)} \end{aligned}$$

On regroupe donc les termes de même signature et on somme sur a (c'est à dire sur les lignes).

Montrons qu'aucune des ces sommes $\sum_{a\in R^n} C_{j1}(a,b)^{e_1}\ldots C_{j_s}(a,b)^{e_s}$ ne dépend de b.

4. Définissons une application affine (de modules) $L : R^n \to R^s$ par la formule

$$L(a) = A_{(J)}a + B_{(J)}b + t_J \text{ où}$$

$J = (j_1,\ldots,j_s)$ est l'ensemble des indices des variables apparaissant dans la signature du terme considéré, $A_{(J)}$ (resp. $B_{(J)}$) est la matrice de format (s,n) avec les lignes $A_{(j_1)},\ldots,A_{(j_s)}$ de A (resp. $B_{(j_1)},\ldots,B_{(j_s)}$ de B) et $t_{(J)} = t_{j_1},\ldots,t_{j_s}$ est le vecteur colonne t limité aux composantes $j_1\ldots j_s$.

En particulier, $A_{(J)}$ représente un homomorphisme de $R^n \to R^s$. Montrons qu'il est surjectif.

Tous les mineurs d'ordre n de A étant des unités de R (par construction de X), toute sous-matrice de format (n,n) de A est inversible (voir 2.9) et définit donc un automorphisme de R^n (voir 2.14).

Soit A' une telle sous-matrice contenant $A_{(J)}$.

Comme on travaille avec des modules libres, tout vecteur $\overrightarrow{v}$ de R^s est combinaison linéaire de vecteurs d'une base (quelconque) de R^s : $\overrightarrow{v} = \sum_{i=1}^{s}\lambda_i e_i$ (voir 2.12). Prolongeons $\overrightarrow{v}$ en un vecteur $\overrightarrow{v'}$ de R^n en lui attribuant n'importe quelle coordonnée pour les $n-s$ dimensions restantes : $\overrightarrow{v'} = \sum_{i=1}^{s}\lambda_i e_i + \sum_{j=s+1}^{n}\mu_j e_j$. Comme A' est un automorphisme $\exists\overrightarrow{u} \mid A'(u) = v'$ (en exprimant $\overrightarrow{u}$ et $\overrightarrow{v'}$ en tant que vecteurs colonnes). Et donc, en se restreignant à R^s, c'est-à-dire en ne considérant que les s lignes $j_1,\ldots,j_s$ de la matrice A', c'est-à-dire $A_{(J)}$, on vient de montrer que $A_{(J)}$ représente une surjection.

5. On peut donc écrire $C_{j_i}(a,b) = q^{j_i-1}N'_{j_i}(L(a)_i)$ (C_{j_i} est défini à partir de la i^{eme} ligne des matrices $A_{(J)}$ et $B_{(J)}$).
Il s'ensuit, par la Proposition 1.5 (voir 3.1.7) que :

$$\sum_{a\in R^n} C_{j_1}(a,b)^{e_1}\ldots C_{j_s}(a,b)^{e_s} = \sum_{a\in R^n}(q^{j_1-1}N'_{j_1}(L(a)_i))^{e_1}\ldots(q^{j_s-1}N'_{j_s}(L(a)_s))^{e_s}$$

$$= q^{e_1(j_1-1)+\ldots+e_s(j_s-1)} \sum_{a\in R^n} (N'_{j_1}(L(a)_1))^{e_1} \ldots (N'_{j_s}(L(a)_s))^{e_s}$$

$$= q^{n-s} q^{e_1(j_1-1)+\ldots+e_s(j_s-1)} (\sum_{i=0}^{q-1} i^{e_1}) \ldots (\sum_{i=0}^{q-1} i^{e_s}) \tag{3.4}$$

Dès lors, cette somme ne dépend pas de b.

On obtient pour $S_b(d)$:

$$S_b(d) = q^n + \sum_{\substack{e_1+\ldots+e_s\leq d \\ e_1,\ldots,e_s\geq 1}} \frac{d!}{e_1!\ldots e_s!} \left(q^{n-s} q^{e_1(j_1-1)+\ldots+e_s(j_s-1)} (\sum_{i=0}^{q-1} i^{e_1}) \ldots (\sum_{i=0}^{q-1} i^{e_s}) \right) \tag{3.5}$$

qui ne dépend pas de b non plus et donc toutes les colonnes ont bien la même somme.

Illustrons cette formule par un exemple numérique :

Travaillons avec un anneau R à 4 éléments et avec la bimagie, donc :
- $q = 4$
- $n = 2$
- M est donc une matrice à $q^2 \times q^2$ éléments, c'est-à-dire 16×16

On doit donc montrer que $S_b(d)$ est égal à la constante de magie simple si $d = 1$ et à la constante de bimagie si $d = 2$.

Calculons d'abord $S_b(1)$:

Comme d est égal à 1, s qui est $\leq d$ ne peut valoir que 1 et donc il n'y aura qu'un seul C_j à la puissance $e_1 = 1$ dans chaque terme. On obtient :

$$\begin{aligned}
S_b(1) &= q^n + \sum_{a\in R} C_1(a,b) + \sum_{a\in R} C_2(a,b) + \sum_{a\in R} C_3(a,b) + \sum_{a\in R} C_4(a,b) \\
&\quad \text{On a } q^{n-s} = q^{2-1} = q \text{ et } q^{e_1(j-1)} = q^{j-1} \text{ et donc} \\
&= q^n + q.q^{1-1} \sum_{i=0}^{3} i + q.q^{2-1} \sum_{i=0}^{3} i + q.q^{3-1} \sum_{i=0}^{3} i + q.q^{4-1} \sum_{i=0}^{3} i \\
&= 16 + 4*6 + 4*4*6 + 4*16*6 + 4*64*6 \\
&= 2056 \text{ qui est bien la constante de la magie simple pour les carrés magiques } 16 \times 16.
\end{aligned}$$

Passons à la bimagie, calculons donc $S_b(2)$:

$$S_b(2) = \sum_{a\in R} \left(1 + \sum_{j=1}^{2n} C_j(a,b) \right)^2$$

Prenons l'exemple du terme $2\sum_{a\in R} C_2(a,b)C_4(a,b)$ qui apparaît dans le développement de la somme ci-dessus. On constate que :
- $s = 2$ (il y a deux C_j).
- $j_1 = 2$ et $j_2 = 4$.

- les deux exposants e_1 et e_2 valent chacun 1.

- $\frac{d!}{e_1!e_2!} = \frac{2!}{1!1!} = 2$

La contribution de ce terme dans le calcul de la formule 3.5 donne donc :

$$2q^{2-2}.q^{1(2-1)}.q^{1(4-1)}(\sum_{i=0}^{q-1} i^1).(\sum_{i=0}^{q-1} i^1) = \quad 2 * 1 * 4 * 64 * 6 * 6 = 18432$$

Les autres termes se calculent de la même manière et on vérifie que le total donne bien la constante de bimagie, à savoir 351576.

Somme sur les lignes

En reprenant, à l'identique le raisonnement ci-dessus, en fixant cette fois-ci une valeur pour a et en faisant varier b, on prouve que les sommes des lignes ont une valeur constante lorsque les éléments de ces lignes sont élevés à la puissance d (avec $1 \leq d \leq n$).

En effet, dans la preuve ci-dessus, on remarque que l'homomorphisme L est symétrique en a et b c'est-à-dire que on peut le définir comme $L(b) = A_{(J)}a + B_{(J)}b + t_J$. La matrice B ayant les mêmes propriétés que la matrice A, on peut appliquer le même raisonnement pour finalement utiliser la Proposition 1.5 qui montre que ces sommes ne dépendent que de q, n et d.

Somme sur la diagonale

Calculons la somme des éléments de la diagonale, chacun élevé à la puissance d ($1 \leq d \leq n$).

$$\sum_{a \in R^n} M^d_{N_n(a), N_n(a)}$$

Reprenons le raisonnement fait sur les colonnes avec cette fois-ci $b = a$.

Définissons une application affine (de modules) $L_1 : R^n \to R^s$ par

$$L_1(a) = A_{(J)}a + B_{(J)}a + t_{(J)} = (A + B)_{(J)}a + t_{(J)}$$

avec $J = (j_1, \ldots, j_s)$ comme précédemment. Puisque tous les mineurs de la matrice $A + B$ sont des unités de R (par construction de X), on voit que, par le même raisonnement que celui fait sur L pour les colonnes, L_1 est surjective. Dès lors, on peut à nouveau utiliser la Proposition 1.5 :

Soit $C_{j_i}(a, a) = q^{j_i - 1} N'_{(j_i)(L_1(a)_i)}$ pour tout $1 \leq i \leq s$. Alors, comme précédemment :

$$\sum_{a \in R^n} C_{j_1}(a,a)^{e_1} \ldots C_{j_s}(a,a)^{e_s} = q^{n-s} q^{e_1(j_1-1)+\ldots+e_s(j_s-1)} (\sum_{i=0}^{q-1} i^{e_1}) \ldots (\sum_{i=0}^{q-1} i^{e_s})$$

Somme sur la contre-diagonale

Remarquons que les indices des éléments de la contre-diagonale sont de la forme $N_n(a), q^n + 1 - N_n(a)$. Calculons la somme des éléments de la contre-diagonale, chacun élevé à la puissance d ($1 \leq d \leq n$).

$$\sum_{a \in R^n} M^d_{N_n(a), q^n + 1 - N_n(a)}$$

C'est ici qu'intervient le fait que les bijections $N_{(j)}$ sont de type c_j. On peut donc appliquer le Lemme 1.3 (voir 3.1.4) : $q^n + 1 - N_n(a) = N_n(-a + c)$.

Définissons l'application affine (de modules) $L_2 : R^n \to R^s$ par

$$L_2(a) = A_{(J)}a + B_{(J)}(-a + c) + t_{(J)} = (A - B)_{(J)}a + (B_{(J)}c + t_{(J)})$$

Remarques :

1. Comme $B_{(J)}$ définit un homomorphisme (voir 2.14), on a le droit de faire $B_{(J)}(-a+c) = B_{(J)}(-a)+B_{(J)}c$.

2. $B_{(J)}c + t_{(J)}$ est un vecteur constant et $(A - B)(J)$ définit un homomorphisme.

Comme $A - B$ a tous ses mineurs d'ordre n dans $U(R)$ (par construction de X), L_2 est donc une application surjective.

On peut donc, comme dans les cas précédents, appliquer la Proposition 1.5.

Les sommes de toutes les colonnes, toutes les lignes et les deux diagonales étant égales, et ce quel que soit la puissance d $(1 \leq d \leq n)$ à laquelle on élève chacun des éléments de la matrice M, on a prouvé que celle-ci est n-multimagique.

CQFD

3.3 Réflexion sur la démonstration

On remarque que dans la démonstration du théorème, les auteurs ont fait le choix de bijections de type c pour les *deux* membres de l'équation 3.2. Or comme expliqué ci-dessus, le caractère de type c de ces bijections n'intervient que pour les *indices* des éléments de la contre-diagonale. c'est-à-dire que seule la bijection N_n du membre de gauche doit être batie sur de telles bijections de type c. En ce qui concerne la bijection N'_{2n} du membre de droite, il s'agit clairement d'une restriction non nécessaire, et que nous pouvons lever. En effet, toute bijection de $R \to \{0, \ldots, q-1\}$ convient pour la définition des N'_{2n}.

Nous verrons au chapitre suivant qu'en levant cette restriction, le nombre de carrés magiques produits par la méthode s'en trouve considérablement augmenté.

Chapitre 4

Discussion sur les paramètres intervenants dans la méthode

Après avoir présenté ce théorème d'existence, encore faut-il choisir les différents éléments intervenant dans celle-ci : quels sont les anneaux à notre disposition, peut-on, avec ceux-ci, construire des matrices génératrices (et combien), quelles sont les bijections utilisables, ... ? Tels sont les questions auquelles ce chapitre répondra.

Avant d'implémenter la méthode, il a fallu de longues réflexions sur les moyens de l'appliquer pour les différents ordres. Nous avons eu besoin d'établir certains résultats concernant les matrices génératrices en rapport avec les anneaux disponibles. Ce chapitre est le fruit de notre tentative de systématisation.

Rappelons l'idée générale de la méthode : si l'on veut construire des carrés n-multimagiques, les ordres des carrés ne sont pas libres : ils doivent être de la forme q^n où q est le cardinal d'un anneau et n le degré de multimagie souhaité.

Comme l'intérêt dans ce travail porte sur la bimagie pour les ordres plus petits ou égal à 23, la méthode peut produire de la bimagie exacte uniquement pour les ordres[1] 9 ($= 3^2$) et 16 ($= 4^2$). Cependant, comme 25 ($= 5^2$) est proche de 23, on étudiera la bimagie pour cet ordre là également.

Par ailleurs, il nous semblé intéressant de porter l'étude sur la magie simple pour laquelle la méthode peut (aux ordres où elle fonctionne, cf *infra*) produire de manière efficace *beaucoup* de carrés magiques. Ensuite, en classant les carrés produits en fonction de leur bimagie partielle, on peut espérer trouver, si pas des carrés bimagiques, du moins des carrés intéressant du point de vue de la bimagie partielle.

Dans une première section, nous étudierons les anneaux disponibles et leurs liens avec les matrices génératrices.

Dans la deuxième section, nous établirons les formules donnant le nombre de bijections utilisables en fonction du cardinal de l'anneau.

Une troisième section parlera du dernier paramètre libre de la méthode, le vecteur t.

Enfin on résumera le chapitre en présentant un tableau estimant le nombre de choix de paramètres possibles pour chaque ordre traité.

[1] rappelons qu'à l'ordre 4, la bimagie n'est pas possible.

4.1 Choix de l'anneau et rapport avec les matrices génératrices

Nous allons donc étudier, pour chaque ordre de carré plus petit ou égal à 25, la possibilité d'utiliser la méthode. Pour cela, nous donnerons les anneaux possibles, puis nous parlerons des matrices génératrices sur ces anneaux. Nous indiquerons le nombre de matrices génératrices différentes pour un anneau donné.

Pour calculer ce nombre, nous avons, à l'aide de notre logiciel, généré toutes les matrices génératrices possibles pour un anneau et un degré de magie donnés. Essentiellement, il s'agit de passer en revue toutes les valeurs possibles pour les éléments d'une matrice de format approprié et de vérifier si la matrice obtenue est génératrice. Nous détaillerons cette idée au chapitre suivant.

Remarquons que si l'on trouve une matrice génératrice, alors on est *sûr* de trouver un carré magique. En effet, comme on l'a remarqué en 3.1.2, il existe toujours au moins *une* bijection de type 1_R.

Nous nous baserons sur un article du mathématicien autrichien Christof Nöbauer, [Small Rings], qui dénombre les anneaux unitaires pour les différents ordres que nous étudions.[2]

Nous serons exhaustifs pour les ordres inférieurs à 8. Pour les ordres, plus grand, il ne nous a pas été possible de recenser tous les anneaux existants.

Pour ces ordres plus grand ou égal à 8, nous avons décidé d'utiliser l'heuristique suivante : si, pour un ordre donné, un corps existe, on le préfèrera aux autres anneaux. En effet, comme le corps contient plus d'unités, il y a plus de possibilité pour choisir des éléments afin de construire une matrice génératrice.
Ce fait sera confirmé pour l'ordre 4, où nous passerons en revue tous les anneaux existants et l'on verra que seul le corps existant pour cet ordre permet de produire des matrices génératrices.

Préalablement, nous allons établir deux résultats qui nous serviront pour prouver la non-existence de matrices génératrices pour certains ordres.

Notation : comme dans le chapitre précédent, une matrice génératrice X sera notée comme juxtaposition de deux matrices A et B : $X = (A\ B)$.
Rappelons que X est de format $(2n, 2n)$ et les matrices A, B de format $(2n, n)$ où n est le degré de multimagie.

Pour la magie simple, une matrice génératrice X est donc de format $(2, 2)$ et les matrices A, B la composant, de format $(2, 1)$.
Pour la bimagie, la matrice génératrice X est de format $(4, 4)$ et les matrices A, B de format $(4, 2)$.

Rappelons également qu'une matrice est génératrice si son déterminant est une unité de l'anneau ainsi que tous les mineurs d'ordre n des matrices A, B, $A + B$ et $A - B$. Pour la magie simple, les mineurs d'ordre 1 sont les éléments de la matrice eux-mêmes tandis que pous la bimagie, il s'agit d'un calcul de déterminant d'une sous-matrice de format $(2, 2)$.

Ci-dessous, ce seront souvent les matrices $A + B$ et $A - B$ qui empêcheront la matrice X d'être génératrice.

[2] Rappelons que nous utilisons des anneaux unitaires dans le cadre de ce travail. Nous nous occuperons donc que de l'existence de tels anneaux aux différents ordres.

4.1.1 Propositions sur les anneaux modulaires

Dans la suite de ce chapitre, nous appellerons *anneau modulaire* un anneau construit sur l'arithmétique modulaire, c'est-à-dire les anneaux $\mathbb{N}/k\mathbb{N},\ k \in \mathbb{N}$. Un anneau modulaire pair est un anneau modulaire dont le cardinal est un nombre pair, donc de la forme $\mathbb{N}/2k\mathbb{N},\ k \in \mathbb{N}$.

Proposition 1

Proposition 1 : Pour les anneaux modulaires pairs et pour la magie simple ($n = 1$), il n'existe pas de matrices génératrices.

Démonstration :

Nous utiliserons le résultat énoncé dans le Chapitre 1 - section Anneau - exemple 2 (voir 2.6), à savoir que les unités de l'anneau $\mathbb{N}/2k\mathbb{N}$ sont les classes dont les représentants sont premiers avec $2k$. Par conséquent, les représentants *pairs* ne sont *pas* des unités de cet anneau.

Comme l'on travaille avec de la magie simple, tous les mineurs d'ordre 1 de la matrice génératrice $X = (A\ B)$ doivent être des unités, donc des nombres impairs.

L'algèbre des anneaux modulaires est telle que la somme (et la différence) de deux nombres impairs donne un nombre pair.

Donc, les mineurs d'ordre 1 de la matrice $A + B$ sont des nombres pairs et ne peuvent, de ce fait, être des unités de l'anneau $\mathbb{N}/2k\mathbb{N}$.

CQFD

Proposition 2

Proposition 2 : Pour les anneaux modulaires dont le cardinal est un multiple de 3, et pour la magie simple ($n = 1$), il n'y a pas de matrices génératrices.

Démonstration :

Comme le cardinal de l'anneau est un multiple de 3, les unités sont les nombres de la forme $3i + 1$ ou $3i + 2$, i étant un nombre naturel. Soient x_1, x_2 deux tels nombres. Deux cas se présentent :

1. Si $x_1 = 3i + 1$ et $x_2 = 3j + 1$ ou si $x_1 = 3i + 2$ et $x_2 = 3j + 2$
   alors leur différence $x_1 - x_2 = 3(i - j)$ est un multiple de 3 et n'est donc pas une unité.

2. Si $x_1 = 3i + 1$ et $x_2 = 3j + 2$ ou si $x_1 = 3i + 2$ et $x_2 = 3j + 1$
   alors leur somme $x_1 + x_2 = 3(i + j) + 1 + 2 = 3(i + j + 1)$ est multiple de 3 et n'est donc pas une unité.

CQFD

Remarquons que ces propositions ne s'appliquent que pour la magie simple puisque, si le degré de multimagie est plus élevé, les mineurs sont les déterminants de sous-matrices d'ordre > 1. On ne peut plus appliquer les raisonnements ci-dessus.

Dans la suite, on va indiquer en fonction de l'ordre du carré souhaité, la possibilité pour la méthode algébrique de produire de la magie simple ou de la bimagie.

Comme l'ordre du carré généré est égal à q^n, q étant le cardinal de l'anneau et n le degré de multimagie, pour la magie simple, le cardinal de l'anneau devra être égal à l'ordre du carré, tandis que pour la bimagie, l'ordre du carré sera le carré du cardinal de l'anneau.

Considérons d'abord différents ordres de carrés pour lesquels nous ne pouvons appliquer la méthode. Ces ordres n'étant pas des carrés parfaits, on ne considérera que la magie simple pour laquelle le cardinal de l'anneau utilisé doit être égale à l'ordre du carré.

4.1.2 Ordres pairs ayant un seul anneau

Les ordres 2, 6, 10, 14, 22 ne disposent que d'un seul anneau, l'anneau modulaire. D'après le Proposition 1 ci-dessus, il n'y aucune matrice génératrice pour ces ordres.

4.1.3 Ordres pairs ayant plusieurs anneaux

D'après [Small Rings], les ordres 12, 18, 20 et 24 possèdent d'autres anneaux. Malheureusement, nous n'avons pu trouver les tables des opérations pour ces anneaux et nous ne savons pas si des matrices génératrices pourraient exister avec ces nouveaux anneaux.

Ces ordres échappent donc (provisoirement ?) à la méthode.

4.1.4 Ordres multiples de 3 ayant un seul anneau

Les ordres 3, 15, et 21 n'ont qu'un seul anneau : l'anneau modulaire.

Nous pouvons appliquer le Proposition 2 ci-dessus pour conclure à la non-existence de matrices génératrices pour ces ordres.

Après ces résultats négatifs, voyons maintenant des ordres pour lesquels la méthode va produire de la magie et/ou de la bimagie.

4.1.5 Ordre 4

Magie simple

$q = 4,\ n = 1$

Quatre anneaux existent :

1. $\mathbb{N}/4\mathbb{N}$. L'arithmétique modulaire. On peut appliquer le Proposition 1 ci-dessus pour conclure qu'aucune matrice génératrice n'existe en utilisant cet anneau.

2. L'anneau donné en l'exemple dans le Chapitre 2 (voir 2.6 exemple 4) que nous reproduisons ici :

$+$	0_R	1_R	a	b
0_R	0_R	1_R	a	b
1_R	1_R	0_R	b	a
a	a	b	0_R	1_R
b	b	a	1_R	0_R

$\times$	0_R	1_R	a	b
0_R	0_R	0_R	0_R	0_R
1_R	0_R	1_R	a	b
a	0_R	a	0_R	a
b	0_R	b	a	1_R

   On remarque que les seules unités sont 1_R et b. On doit donc les choisir comme éléments des matrices A et B. Mais leur somme donne 0 ou a qui ne sont pas des unités. Donc il n'y a pas de matrice génératrice avec cet anneau.

3. Voici un autre anneau :

$+$	0_R	1_R	a	b
0_R	0_R	1_R	a	b
1_R	1_R	0_R	b	a
a	a	b	0_R	1_R
b	b	a	1_R	0_R

$\times$	0_R	1_R	a	b
0_R	0_R	0_R	0_R	0_R
1_R	0_R	1_R	a	b
a	0_R	a	a	0_R
b	0_R	b	0_R	b

   On constate que seul 1_R est unité. Dès lors, tous les éléments de la matrices A et B doivent valoir 1_R et leur différence fait 0_R. Donc cet anneau n'est pas utilisable non plus pour trouver des matrices génératrices.

4. Enfin, un corps existe. Il a été décrit dans le Chapitre 2 (voir 2.7 - exemple 3). Les tables de ses opérations sont :

$+$	0_R	1_R	a	b
0_R	0_R	1_R	a	b
1_R	1_R	0_R	b	a
a	a	b	0_R	1_R
b	b	a	1_R	0_R

$\times$	0_R	1_R	a	b
0_R	0_R	0_R	0_R	0_R
1_R	0_R	1_R	a	b
a	0_R	a	b	1_R
b	0_R	b	1_R	a

   Avec ce corps-ci, nous trouvons des matrices génératrices, comme indiqué au Chapitre 3 dans lequel nous donnions un exemple d'une telle matrice. En voici une autre :

$$X = \begin{pmatrix} a & b \\ a & 1_R \end{pmatrix}$$

   En testant toutes les possibilités pour chacun des éléments de la matrice X, on trouve qu'il y a 18 matrices génératrices pour cet anneau.

Bimagie

$q = 2,\ n = 2$

Le lecteur attentif aura remarqué que 4 est un carré parfait, donc nous pouvons nous demander si il peut y avoir de la bimagie pour cet ordre.

Au Chapitre 1 (voir 1.2.1), nous avons prouvé qu'il ne pouvait exister de carrés bimagiques pour cet ordre.

Mais pourrait-on trouver des matrices génératrices ? Non, bien sûr ! Le contre-exemple donné au chapitre précédent (voir 3.2.2 exemple 3) explique pourquoi il ne peut exister de matrice X de format $(4, 4)$ en utilisant l'anneau $\mathbb{N}/2\mathbb{N}$.

4.1.6 Ordre 5

Magie simple

$q = 5,\ n = 1$

Il n'y a qu'un seul anneau pour l'ordre 5 : le corps $\mathbb{N}/5\mathbb{N}$.

Il y a 32 matrices génératrices pour cet anneau. En voici un exemple :

$$X = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$$

4.1.7 Ordre 7

Magie simple

$q = 7,\ n = 1$

Le seul anneau est le corps $\mathbb{N}/7\mathbb{N}$. Avec celui-ci, il existe 432 matrices génératrices. Donnons une de celles-ci :

$$X = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$$

Remarquons qu'il s'agit de la même matrice que celle donnée en exemple pour l'ordre 5. Mais, attention, les opérations algébriques ne sont pas les mêmes : dans un cas, on utilise l'arithmétique modulo 5 et dans l'autre l'arithmétique modulo 7.

4.1.8 Ordre 8

Magie simple

$q = 1,\ n = 1$

Comme indiqué dans l'introduction de cette section, à partir de l'ordre 8, nous ne pourrons plus être exhaustif concernant les anneaux.

Remarquons tout d'abord que nous ne pouvons utiliser l'anneau modulaire puisqu'il est pair et tombe sur

le coup du Proposition 1.

Mais, il existe un corps dont voici les tables des opérations algébriques.
Remarque : nous noterons dorénavant les éléments des corps 0,1,2,...plutôt que $a, b, \ldots$ Noublions cependant pas qu'il ne s'agit pas de "vrais" nombres. Par exemple, les tables ci-dessous nous indiquent que $1 + 1 = 0$ et $2 * 4 = 3$!

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

A l'aide de ce corps, nous trouvons 1 470 matrices génératrices.

Remarque sur la trimagie

$q = 2,\ n = 3$

Comme 8 est le premier cube parfait ($= 2^3$), demandons-nous si on peut construire une matrice génératrice $X = (A\ B)$ de format $(6, 6)$ sur le corps $\mathbb{N}/2\mathbb{N}$.

Si on en trouvait une, nous pourrions construire des carrés trimagiques et par force bimagiques d'ordre 8. Malheureusement, ce n'est pas possible car il existe une preuve de non existence de trimagie pour les ordres inférieurs à 12 (voir [Site Multimagie]). Par ailleurs, comme nous l'avons déjà fait (voir à nouveau 3.2.2 exemple 3), il est également possible de montrer l'inexistence d'une matrice A, de format $(6, 3)$ tel que tous ses mineurs d'ordre 3 soient non nuls.

4.1.9 Ordre 9

Magie simple

$q = 9,\ n = 1$

L'anneau modulaire n'est pas utilisable puisque 9 est un multiple de 3 et donc par le Proposition 2 ci-dessus, aucune matrice génératrice n'existe avec cet anneau.

Cependant, il existe un corps puisque $9 = 3^2$, 3 étant un nombre premier (voir 2.7 exemple 4). Voici ses

tables :

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	7	2	0	1	5	3	4

×	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	2	5	8	1	4	7
4	0	4	8	5	6	1	7	2	3
5	0	5	7	8	1	3	4	6	2
6	0	6	3	1	7	4	2	8	5
7	0	7	5	4	2	6	8	3	1
8	0	8	4	7	3	2	5	1	6

Grâce à ce corps, nous obtenons 1.920 matrices génératrices.

Bimagie

$q = 3,\ n = 2$

Comme 9 est un carré parfait, la méthode permet de construire des carrés bimagiques pour autant que nous puissions trouver des matrices génératrices.

Nous travaillons avec le corps à trois éléments ($q = 3$) et nous devons trouver des matrices génératrices de format $(4, 4)$. Il faut donc que les mineurs d'ordre 2 des matrices A, B, $A + B$, $A - B$ soient non nuls.

Il existe 2 304 matrices répondant à ces conditions. Exemple d'une telle matrice génératrice :

$$X = \begin{pmatrix} 2 & 2 & 2 & 1 \\ 2 & 1 & 1 & 1 \\ 2 & 0 & 0 & 2 \\ 0 & 2 & 1 & 0 \end{pmatrix}$$

On remarque bien qu'ici des zéros apparaissent dans la matrice mais, ce sont les déterminants de matrice de format $(2, 2)$ qui doivent être des unités, pas les éléments eux-mêmes.

Cependant, il n'y a "que" 2 304 matrices génératrices. Ceci est dû au fait que l'anneau utilisé ne contient que 3 éléments. Nous verrons au chapitre suivant le choix algorithmique que nous faisons lorsque nous voulons produire aléatoirement des matrices génératrices de ce type.

4.1.10 Ordre 11

Magie simple

$q = 11,\ n = 1$

Le seul anneau est le corps $\mathbb{N}/11\mathbb{N}$. Il existe 5 600 matrices génératrices avec ce corps.

4.1.11 Ordre 13

Magie simple

$q = 13,\ n = 1$

Le seul anneau est le corps $\mathbb{N}/13\mathbb{N}$. Il existe 12 960 matrices génératrices avec ce corps.

4.1.12 Ordre 16

Magie simple

$q = 16,\ n = 1$

Nous donnons ci-dessous l'algèbre du corps à 16 éléments.

La loi + :

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
2	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

La loi $\times$:

$\times$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
4	0	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
5	0	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
6	0	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
7	0	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
8	0	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
9	0	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
10	0	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
11	0	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
12	0	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
13	0	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
14	0	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
15	0	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

Nous produisons 40 950 matrices génératrices avec ce corps.

Bimagie

$q = 4,\ n = 2$

Dans ce cas-ci, nous devons prendre un anneau de cardinal 4 et créer des matrices génératrices de format $(4, 4)$. *A priori* tous les anneaux pourraient nous en fournir puisque, comme indiqué plus haut, dans le cas de la bimagie, la Proposition 1 ne peut s'appliquer.

Cependant des essais nous ont montré que dans ce cas également, seul le corps à 4 éléments nous fournissait des matrices génératrices.

Nous en avons répertorié 5 715 360

En voici une :

$$X = \begin{pmatrix} 3 & 3 & 1 & 0 \\ 2 & 0 & 3 & 3 \\ 1 & 2 & 0 & 3 \\ 0 & 3 & 1 & 3 \end{pmatrix}$$

Comme pour la bimagie de l'ordre 9, rien n'empêche des zéros d'apparaître. Ceci explique qu'on trouve beaucoup de matrices génératrices.

4.1.13 Ordre 17

Magie simple

$q = 17,\ n = 1$

Le seul anneau est le corps $\mathbb{N}/17\mathbb{N}$. Il existe 46 592 matrices génératrices avec ce corps.

4.1.14 Ordre 19

Magie simple

$q = 19,\ n = 1$

Le seul anneau est le corps $\mathbb{N}/19\mathbb{N}$. Il existe 77 760 matrices génératrices avec ce corps.

4.1.15 Ordre 23

Magie simple

$q = 23,\ n = 1$

Le seul anneau est le corps $\mathbb{N}/23\mathbb{N}$. Il existe 183 920 matrices génératrices avec ce corps.

4.1.16 Ordre 25

Magie simple

$q = 25,\ n = 1$

Plusieurs anneaux existent mais nous pouvons cette fois-ci, et pour la première fois utiliser l'anneau modulaire malgré qu'il ne soit pas un corps. En effet, il y a suffisement d'éléments dans l'anneau pour construire des matrices génératrices. La première de celles-ci est :

$$X = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

Il y a en tout 20 000 matrices génératrices avec cet anneau. On remarque avec cet ordre que notre heuristique semble correcte : il n'y a "que" 20 000 matrices génératrices pour l'ordre 25 alors qu'il y en a 183 920 pour l'ordre 23. A l'ordre 23 nous utilisions un corps tandis qu'ici il s'agit d'un anneau.

Bimagie

$q = 5,\ n = 2$

A l'aide du corps $\mathbb{N}/5\mathbb{N}$, on construit des matrices génératrices.

Exemple d'une telle matrice :

$$X = \begin{pmatrix} 2 & 2 & 1 & 4 \\ 3 & 4 & 2 & 2 \\ 0 & 1 & 1 & 2 \\ 2 & 4 & 0 & 4 \end{pmatrix}$$

Nous dénombrons 277 585 920 matrices génératrices.

4.2 Choix des bijections

Nous allons étudier dans cette section la combinatoire des bijections utilisées dans la méthode.

Dans le Théorème 2.2 du chapitre précédent, nous utilisions des bijections de type c pour calculer les indices des éléments dans le membre de gauche de l'équation 3.2. Et, suivant la remarque de la fin du chapitre, nous ne sommes pas limités à ces bijections de type c pour le membre de droite.

4.2.1 Nombre de bijections de type c

Le nombre de bijections de type c pour un anneau R donné, contenant q éléments est calculable.

Le Lemme 1.2 du chapitre précédent (voir 3.1.2) donne une méthode de construction pour les bijections de type c. Le but du lemme en question était cependant de montrer *l'existence* d'une telle bijection.

Ici, nous allons montrer comment calculer (et construire) *toutes* les bijections de type c pour un anneau.

Selon le lemme, deux cas peuvent se présenter :

- **Premier cas :** 2_R est une unité de l'anneau[3] .

  Il existe alors des bijections de type c pour tout élément c de l'anneau.

  Notons, dans ce cas, $s = (q-1)/2$ où q est comme d'habitude le cardinal de l'anneau.

  Pour chaque élément c_i, calculons le nombre de bijections de type c_i que nous pouvons contruire.

  Puisque 2_R est une unité, il y a un élément a_0 qui est point fixe de l'application φ_{c_i} (rappel : $\varphi_{c_i}(a) = -a + c_i,\ \forall a \in R$).
  Les s autres éléments ont une orbite à deux éléments. Ils sont regroupés en couple, c'est-à-dire que la valeur de l'un impose une valeur pour son "binôme" :

  $N(\varphi_{c_i}(a_k)) = q - 1 - N(a_k)$ pour $k \in \{1, \ldots, s\}$

  Il y a $q-1$ manières de donner une valeur à $N(a_1)$ (puisque $N(a_0)(= s)$ est fixé), $q-3$ pour $N(a_2)$,

[3] rappelons encore une fois que nous travaillons avec des anneaux quelconques et qu'il ne faut pas se laisser abuser par les représentations numériques de ceux-ci. 2_R représente l'élément $1_R + 1_R$.

..., $q-(2s-1)$ pour $N(a_s)$. Donc

$$\begin{aligned} \textit{Nombre de bijections de type } c_i &= 1.(q-1).(q-3)\ldots(q-(2s-1)) \\ &= (q-1).(q-3)\ldots 2 \\ &= \Pi_{j=1}^{s} 2j \end{aligned}$$

Comme nous pouvons prendre les q éléments de l'anneau comme c_i, le nombre total de bijection de type c pour cet anneau est donc finalement :

$$\textit{Nombre de bijections de type } c = q.\Pi_{j=1}^{s} 2j \tag{4.1}$$

- **Second cas :** 2_R n'est pas une unité de l'anneau.

Dans ce cas, il n'y a de bijection de type c que pour les unités de l'anneau. Soit c_i une telle unité[4].

Il n'y a pas de point fixe pour l'application φ_{c_i}.

Notons $s = q/2$

En reprenant le raisonnement précédent, on a q choix pour $N(a_1)$, $q-2$ pour $N(a_2)$, ..., $q-2(s-1)$ pour $N(a_s)$.

$$\begin{aligned} \text{Nombre de bijections de type } c_i &= q.(q-2)\ldots(q-2(s-1)) \\ &= (q).(q-2)\ldots 2 \\ &= \Pi_{j=1}^{s} 2j \end{aligned}$$

Si $\#U(R) = q_{unites}$, alors le nombre total de bijections de type c est égal à :

$$\textit{Nombre de bijections de type } c = q_{unites}.\Pi_{j=1}^{s} 2j \tag{4.2}$$

4.2.2 Nombre de bijections quelconques

Dans le membre de droite de l'équation du Théorème 2.2, il n'est pas nécessaire d'utiliser des bijections de type c pour construire la bijection N'_{2n}.

Dès lors, toute bijection de $R \to \{0, \ldots, q-1\}$ convient. Comme R contient q éléments, il y a $q!$ bijections.

[4]puisque nous travaillons avec des anneaux unitaires, nous sommes assurés que l'ensemble $U(R)$ contient au moins 1 élément.

Il y a donc sensiblement plus de bijections quelconques que de bijections de type c.

Remarquons que nous "gagnons" deux fois parce que nous avons besoin de n bijections de type c pour le membre de gauche, mais de $2n$ bijections (quelconques) pour le membre de droite.

4.3 Choix du vecteur t

Le dernier paramètre à faire varier est le vecteur t apparaissant dans le membre de droite de l'équation du Théorème 2.2. Ce vecteur est de dimension $2n$ (n étant le degré de multimagie) et prend ses valeurs dans l'anneau R de cardinal q.

Pour un carré magique d'ordre q^n, il y a donc q^{2n} vecteurs t différents, c'est-à-dire le nombre d'éléments du carré magique.

Par exemple, pour l'ordre 5, il y a $5^2 = 25$ vecteurs t différents, pour l'ordre 16 il y en a $16^2 = 256$, etc ...

4.4 Tableau récapitulatif

Nous allons résumer toutes ces informations dans un tableau récapitulatif.

Chaque ligne de ce tableau comprend l'ordre du carré, l'anneau utilisé, le nombre de matrices génératrices avec cet anneau, le nombre de bijections de type c différentes que l'on peut utiliser pour construire la bijection N_n du membre de gauche de l'équation du théorème 2.2, le nombre de permutations utilisées dans le membre de droite de cette équation, le nombre de vecteurs t et enfin le nombre total de configurations possibles en faisant le produit de toutes les colonnes précédentes.

Concernant les bijections, rappelons que l'on a besoin de n bijections (de type c) pour construire la bijections N_n du membre de gauche et de $2n$ bijections pour construire la bijection N_{2n} du membre de droite de l'équation 3.2.

Le nombre total de possibilités ne veut *pas* dire qu'il y autant de carrés magiques ou bimagiques différents. En effet, il y a forcément une certaine redondance entre ces paramètres. Pour un ordre donné, telle matrice génératrice avec tel vecteur t en utilisant telles bijections pourrait produire le même carré[5] qu'un autre ensemble de paramètres. Il est difficile, mais selon nous pas impossible, de déterminer les ensembles de paramètres qui produisent le même carré. Cependant, nous n'avons pu mener ce travail.

On constate que le nombre de possibilité augmente exponentiellement.

C'est pour cette raison qu'il n'est pas envisageable de générer systématiquement, hormis pour les tout petits ordres, toutes les possibilités. Même si la méthode est de complexité algorithmique polynomiale pour générer un carré (voir chapitre suivant), c'est l'espace de solutions qui est hautement exponentiel.

Sachant cela, dans le chapitre suivant, nous adopterons une approche stochastique pour choisir les paramètres.

[5] nous avons choisi de considérer comme égaux deux carrés ayant les mêmes termes aux mêmes places. D'autres choix existent dans la littérature.

Ordre du carré	Degré de multimagie	Anneau	Nb matrices génératrices I	Nb Bijections de type c II	Nb Bijections quelconques III	Vecteur t IV	Total $= I * II * III * IV$
2	1	$\mathbb{N}/2\mathbb{N}$	0	-	-	-	0
3	1	$\mathbb{N}/3\mathbb{N}$	0	-	-	-	0
4	1	Corps	18	$= 3 * 8 = 24$	$(4!)^2 = 576$	16	3 981 312
4	2	$\mathbb{N}/2\mathbb{N}$	0	-	-	-	0
5	1	$\mathbb{N}/5\mathbb{N}$	32	$5 * 8 = 40$	$(5!)^2 = 14400$	25	460 800 000
6	1	$\mathbb{N}/6\mathbb{N}$	0	-	-	-	0
7	1	$\mathbb{N}/7\mathbb{N}$	432	$7 * 48 = 336$	$(7!)^2 = 25401600$	49	180 667 559 116 800
8	1	Corps	1 470	$7 * 384 = 2\,688$	$(8!)^2 > 1,6\ 10^9$	64	$> 400\ 10^{15}$
8	3	$\mathbb{N}/2\mathbb{N}$	0	-	-	-	0
9	1	Corps	1 920	$9 * 384 = 3\,456$	$(9!)^2 > 1,3\ 10^{11}$	81	$> 70\ 10^{18}$
9	2	$\mathbb{N}/3\mathbb{N}$	2 304	$(3 * 2)^2 = 36$	$(3!)^4 = 1\,296$	81	8 707 129 344
10	1	$\mathbb{N}/10\mathbb{N}$	0	-	-	-	0
11	1	$\mathbb{N}/11\mathbb{N}$	5 600	$11 * 3840 = 42\,240$	$(11!)^2 > 1,5\ 10^{15}$	121	$> 42\ 10^{24}$
12	1	$\mathbb{N}/12\mathbb{N} + ?$	0	-	-	-	0
13	1	$\mathbb{N}/13\mathbb{N}$	12 960	$13 * 46080 = 599\,040$	$(13!)^2 > 38\ 10^{18}$	169	$> 50\ 10^{30}$
14	1	$\mathbb{N}/14\mathbb{N}$	0	-	-	-	0
15	1	$\mathbb{N}/15\mathbb{N}$	0	-	-	-	0
16	1	Corps	40 950	$15 * 10\,321\,920 = 154\,828\,800$	$(16!)^2 > 437\ 10^{24}$	256	$> 1,7\ 10^{37}$
16	2	Corps à 4 éléments	5 715 360	$(3 * 8)^2 = 576$	$(4!)^4 = 331\,776$	256	$> 279\ 10^{15}$
17	1	$\mathbb{N}/17\mathbb{N}$	46 592	$17 * 10\,321\,920 = 175\,472\,640$	$(17!)^2 > 126\ 10^{27}$	289	$> 2\ 10^{44}$
18	1	$\mathbb{N}/18\mathbb{N} + ?$	0	-	-	-	0
19	1	$\mathbb{N}/19\mathbb{N}$	77 760	$19 * 185\,794\,560 = 3\,530\,096\,640$	$(19!)^2 > 126\ 10^{27}$	289	$> 1,2\ 10^{52}$
20	1	$\mathbb{N}/20\mathbb{N} + ?$	0	-	-	-	0
21	1	$\mathbb{N}/21\mathbb{N}$	0	-	-	-	0
22	1	$\mathbb{N}/22\mathbb{N}$	0	-	-	-	0
23	1	$\mathbb{N}/19\mathbb{N}$	183 920	$23 * 3\,715\,891\,200 = 85\,465\,497\,600$	$(23!)^2 > 6,6\ 10^{44}$	529	$> 5,5\ 10^{63}$
24	1	$\mathbb{N}/24\mathbb{N} + ?$	0	-	-	-	0
25	1	$\mathbb{N}/25\mathbb{N}$	20 000	$25 * 89\,181\,388\,800 = 2\,229\,534\,720\,000$	$(25!)^2 > 2,4\ 10^{50}$	625	$> 6,7\ 10^{69}$
25	2	$\mathbb{N}/5\mathbb{N}$	277 585 920	$(5 * 8)^2 = 1\,600$	$(5!)^4 = 8\,918\,138\,880\,000$	625	$> 2,4\ 10^{27}$

Chapitre 5

Implémentation logicielle

Lorsqu'il s'agit d'implémenter un algorithme, des choix de langage, d'architecture et de structure de données doivent être faits.

Nous passerons notre code en revue et nous en extrairons les éléments qui nous paraissent nécessiter quelques explications.

5.1 Fonctionnalités du logiciel

Le logiciel a pour fonctionnalité principale la génération de carrés magiques et bimagiques.

En fonction du degré de magie choisi par l'utilisateur, le système propose un choix d'ordre de carré.

Lorsque l'utilisateur choisi d'étudier la magie simple, le système classe les carrés magiques générés en fonction de leur degré de bimagie partielle.

Pour la génération d'un carré, des paramètres doivent être choisi par le système (voir Chapitre précédent). Comme la combinatoire de ceux-ci est gigantesque, le système fonctionne de manière stochastique quant à leur sélection.

L'utilisateur peut décider du nombre d'essais de génération effectués par le système.

L'utilisateur peut également choisir le nombre de résultats qu'il veut garder en mémoire.

L'utilisateur peut naviguer dans l'ensemble des carrés produits. Ils sont classés en fonction de leur score de bimagie partielle.

L'utilisateur a la possibilité d'interrompre une recherche lancée, puis de la reprendre.

L'utilisateur a deux possibilités de stockage sur disque. Un format natif lui permet, dans une session ultérieure, de recharger en mémoire vive le travail en l'état.
Il peut également exporter les résultats dans un format texte lui laissant l'opportunité de les exploiter dans un autre logiciel (un tableur par exemple).

5.2 Langage

Nous avons opté pour un langage généraliste orienté objet permettant la réalisation aisée d'une interface utilisateur graphique.

Par ailleurs, comme nous ne voulions pas nous limiter à une seule plate-forme d'exploitation, il nous a semblé naturel de développer ce logiciel dans le langage Java.

Nous avons utilisé la version 1.6 de ce langage.

5.3 Architecture générale

Le paradigme de développement utilisé est le modèle orienté objet.

L'architecture du logiciel respecte un standard en vigueur, à savoir l'architecture Modèle - Vue - Contrôleur.

Il nous a, en effet, semblé important de séparer les responsabilités dans différentes classes distinctes dans leurs fonctionnalités.

Dans le cadre de ce mémoire, nous concentrerons principalement les explications sur la partie 'Modèle' de l'application. C'est évidemment dans cette partie que se trouvent les classes implémentant la méthode algébrique décrite dans les chapitres précédants.

Avant de passer à l'étude de ces classes, disons un mot sur le multi-threading[1] utilisé dans le programme.

Comme l'utilisateur peut lancer le programme dans de longues recherches, il nous a paru souhaitable qu'il puisse exploiter les résultats au fur et à mesure qu'ils sont produits par le système.

Nous avons donc décidé de lancer le module de génération dans un thread séparé afin de permettre à l'utilisateur de "garder la main" sur le reste du programme.

Pour ce faire, les deux threads (le thread de l'utilisateur et le thread du moteur de génération) partagent une structure de donnée qui est modifiée par le thread de génération et lue par le thread utilisateur. Nous expliquerons ci-dessous quel a été le choix technique retenu.

5.4 Moteur de génération

Le programme de génération de carré est essentiellement une boucle sur le nombre d'essais demandés par l'utilisateur. A intervalle régulier, ce thread vérifie si il n'a pas été interrompu. Il est, en effet, de bonne programmation de ne pas interrompre un thread autoritairement mais plutôt de demander à celui-ci de s'arrêter ; ce qui lui permet de ne pas se trouver dans un état incohérent ce qui rendrait le programme instable et incontrôlable (voir [Horstmann 2002] Ch 1).

[1] le multi-threading est le procédé par lequel un programme est décomposé en sous-parties, appelées *threads*, qui, chacune reçoit du système d'exploitation une fenêtre de temps pour s'exécuter. Il s'agit d'un mécanisme pour implémenter les aspects multitâches au sein d'un même programme. Pour une introduction de l'utilisation des threads en Java, voir [Horstmann 2002]

Avant de rentrer dans la boucle susmentionnée, le programme initialise certains paramètres :

1. Sélection d'un anneau via la *factory* d'anneau (voir *infra*).

2. Obtention d'une *factory* de matrices génératrices (voir *infra*).

3. Initialisation d'un vecteur t.

A chaque itération de la boucle, le programme de génération choisit aléatoirement un ensemble de bijections, une matrice génératrice ainsi qu'une valeur pour le vecteur t.

Un nouveau carré magique est alors construit à l'aide de ces paramètres.

Dans le programme, un carré magique est une matrice. Pour remplir cette matrice, on utilise deux boucles imbriquées chacune d'elles parcourant les q^n éléments du module à n dimensions sur l'anneau utilisé. Pour fixer les idées, appelons a le vecteur de la boucle extérieure et b celui de la boucle intérieure.

On calcule pour chaque couple de vecteurs (a, b) :

1. Les indices de la matrice déterminant l'élément de celle-ci auquel on affectera une valeur. On utilise une fonction de l'anneau pour faire ces calculs d'indice (voir plus bas).

2. Le produit matriciel de la matrice génératrice et de la concaténation des vecteurs a et b.

3. La somme du produit matriciel et du vecteur t.

4. A partir du résultat précédent, on obtient la valeur à affecter à l'élément de la matrice via la même méthode de l'anneau (mais utilisant des paramètres de bijections différents).

5. Un fois le carré magique produit, on calcule le degré de bimagie partielle afin de classer ce carré. Dans le cas de bimagie exacte (ordres 9, 16 et 25), ce calcul ne prête à aucune conséquence puisque tous les carrés obtiennent la même valeur (maximale) pour ce critère.

6. Le carré est ajouté (si possible, voir plus loin) à la structure de donnée contenant l'ensemble des carrés déjà produits.

5.5 Anneaux et *Factory* d'anneaux

5.5.1 Classe RingFactory

La classe 'RingFactory' a pour tâche de fournir un anneau valide en fonction de l'ordre du carré souhaité et du degré de multimagie (magie simple ou bimagie).

Le nom 'Factory' provient du fait que cette classe implémente le *design pattern Factory*, à savoir l'idée qu'une classe particulière s'occupe de fournir des objets d'un certain type pour le reste du programme[2]. Ici, la *factory* construira un objet d'une classe spécialisant la classe 'Ring'.

5.5.2 Classe Ring

La classe 'Ring' a pour responsabilité le bon fonctionnement de l'anneau. Elle offre les fonctionnalités principales suivantes :

1. Les opérations algébriques $+$ et $\times$

2. Le calcul des bijections N_n et N_{2n}.

3. La sélection de bijections (de type c ou non) utilisées par les deux bijections précitées.

Une bijection de type c est représentée à l'aide d'un tableau d'entiers à q dimensions prenant ses valeurs dans l'ensemble $\{0, \ldots, q-1\}$.

Voici l'algorithme utilisé pour construire une bijection de type c.

[2]une explication de ce *design pattern* est donnée dans [Metsker 2006] Ch. 16.

initialiser un tableau $tabBij$ de q éléments avec la valeur -1
initialiser un tableau $tabValeurs$ de q éléments avec les valeurs $\{0, \ldots, q-1\}$
si $1_R + 1_R \in R$ *alors*
    choisir c parmi les q éléments de R
    $a_0 := 2^{-1}c$
    $s := (q-1)/2$
    $tabBij[a_0] := s$
    $tabValeurs := tabValeurs \setminus \{s\}$
sinon
    $s := q/2$
    choisir c parmi $U(R)$
fin si
pour i *de 1 à* s *faire*
    choisir a_k tel que $tabBij[a_k] = -1$
    $ind_{binone} := -a_k + c$
    choisir val_1 parmi $tabValeurs$
    $val_2 := q - 1 - val_1$
    $tabBij[a_k] := val_1$
    $tabBij[ind_{binome}] := val_2$
    $tabValeurs := tabValeurs \setminus \{val_1, val_2\}$
fin pour
retourner $tabBij$

Cet algorithme est de complexité quadratique $O(q^2)$ (puisqu'il y a en fait deux boucles imbriquées, une de 1 à s et une pour choisir les valeurs disponibles, les deux boucles étant d'ordre q).

En fonction de l'ordre utilisé, deux stratégies de sélection des bijections de type c sont utilisées :

1. Pour les petits ordres, on stocke (en mémoire vive) lors de la construction de l'objet 'Ring' un tableau (de tableaux) contenant toutes les bijections de type c possibles. On utilise l'algorithme ci-dessus pour construire chacune des bijections de type c possibles. Dans ce cas, la méthode 'choisir' de cet algorithme parcourt d'une manière systématique les valeurs disponibles.

   La sélection aléatoire d'une bijection de type c consiste simplement à choisir au hasard un élément de ce tableau de tableaux.

   Le travail de construction de ces bijections est compensé par un accès plus rapide lors de la génération des carrés.

2. Pour les ordres plus importants, le nombre de bijections de type c devenant trop important, on construit celles-ci à la "volée". La méthode 'choisir' sélectionne aléatoirement une valeur disponible.

En ce qui concerne les bijections quelconques, elles sont générées à la volée en utilisant l'algorithme de complexité linéaire $O(q)$ suivant :

initialiser un tableau $tabBij$ de q éléments avec les valeurs $\{0, \ldots, q-1\}$
pour i *de* 0 *à* $q-1$ *faire*
    choisir aléatoirement j entre i et $q-1$
    échanger $tabBij[i]$ et $tabBij[j]$
fin pour
retourner $tabBij$

Classes spécialisant Ring

Différentes classes spécialisent 'Ring' : 'Ring4', 'Ring8', 'Ring9' et 'Ring16'.

Les seules méthodes qui sont redéfinies dans ces classes sont celles qui concernent les opérations algébriques.

5.6 Matrice et Carré magique

Dans tout ce travail, un carré magique est vu comme une matrice. C'est donc de cette façon que nous l'avons implémenté.

5.6.1 Classe Matrice

Dans notre logiciel, la classe 'Matrice' est responsable :

- Du stockage des nombres composant un objet de cette classe.
- Du stockage de l'anneau utilisé.
- Des opérations matricielles telles que l'addition, la soustraction, le produit matriciel.
- D'une opération d'égalité qui teste si deux matrices sont égales. Deux matrices sont égales si elles ont les mêmes valeurs pour les mêmes indices.
- D'opérations spécifiques à notre problématique ; parmi celles-ci : la juxtaposition de deux matrices, la séparation d'une matrice en sous-matrices, l'affectation aléatoire ou systématique de valeurs pour les différents indices.

5.6.2 Classe CarreMagique

La classe 'CarreMagique' étend la classe 'Matrice'.

Le constructeur de cette classe reçoit les paramètres (anneau, matrice génératrice, vecteur t) lui permettant de construire le carré magique.

Un objet de cette classe connait également son score de bimagie partielle.

C'est sur base de ce dernier qu'elle implémente une méthode 'compareTo' utile pour classer les carrés magiques produits.

5.7 Générateur de matrices génératrices

La classe 'MatriceXGen' sert à fournir des matrices génératrices à la demande via la méthode 'getNextMatriceX'. La matrice retournée par cette méthode est choisie aléatoirement.

Selon le degré de magie souhaité, les matrices génératrices sont soit fabriquées par le constructeur et stockées dans un tableau (si $n = 1$ ou $n = 2$ pour l'ordre 9), soit construites à la volée lors de la demande (si $n = 2$ pour les ordres 16 et 25). En effet, le temps de construction d'une matrice génératrice peut être relativement long et si l'on fait beaucoup d'itérations de la boucle principale du programme, mieux vaut construire ces matrices une fois pour toutes.

Il y a deux algorithmes de construction des matrices génératrices : l'un, stochastique, pour le mode "à la volée", l'autre, systématique, pour le stockage dans un tableau.

Voici une description de l'algorithme utilisé.

Notations :

- On appelera matrice *unitaire* une matrice dont le déterminant est une unité de l'anneau.
- on dira que deux matrices $M1$ et $M2$, chacune de format (n, n), sont compatibles si la matrice

$$M = \begin{pmatrix} M1 \\ M2 \end{pmatrix}$$

  juxtaposition (verticale) de $M1$ et $M2$, de format $(2n, n)$ est telle que tous ses mineurs d'ordre n soient des unités de l'anneau R.

1. Découpons la matrice génératrice X en 4 sous-matrices de format (n, n).

$$X = \begin{pmatrix} A1 & B1 \\ A2 & B2 \end{pmatrix}$$

2. L'idée est de chercher d'abord une sous-matrice $A1$ unitaire (au sens défini ci-dessus).

3. Chercher de la même manière une sous-matrice $A2$ unitaire, qui, de plus est compatible avec $A1$.

4. Chercher une sous-matrice $B1$ unitaire.

5. Chercher une matrice $B2$, unitaire, compatible avec $B1$.

6. Juxtaposer $A1$ et $A2$ ainsi que $B1$ et $B2$:

$$A = \begin{pmatrix} A1 \\ A2 \end{pmatrix} \qquad B = \begin{pmatrix} B1 \\ B2 \end{pmatrix}$$

7. Verifier que tous les mineurs d'ordre n des matrices $A + B$ et $A - B$ soient des unités de R.

8. Vérifier que la matrice X ainsi construite est unitaire.

Remarques :

- La dernière vérification est nécessaire car les étapes précédentes sont 'locales' et ne garantissent pas que le déterminant de X est une unité.

- Cet algorithme de découpage en 4 blocs est *beaucoup* plus efficace qu'une génération aléatoire de tous les éléments de la matrice X et de vérifier ensuite si la matrice ainsi obtenue est génératrice.

  Pour la bimagie à l'ordre 9, c'est-à-dire donc en utilisant l'anneau à 3 éléments $\mathbb{N}/3\mathbb{N}$, l'algorithme décrit est environ 100 fois plus rapide.

- Lorsque cet algorithme s'utilise pour la construction aléatoire d'une matrice génératrice, les choix des éléments dans les différents blocs sont eux-mêmes aléatoires. Par contre, si on veut construire toutes les matrices génératrices pour les stocker dans un tableau, on parcourt chaque bloc de manière systématique.

5.8 Structure de stockage des carrés générés

Les carrés générés par le thread que nous avons appelé *moteur de génération* sont stockés (en mémoire vive) dans une structure de donnée qui est lue par le thread utilisateur aux fins d'affichage, de sauvegarde sur disque, etc ...Nous utilisons une structure de donnée qui implémente la notion d'ensemble. En effet, comme déjà indiqué, notre logiciel pourrait générer des carrés identiques. En utilisant une structure ensembliste, nous nous prémunissons de doublons éventuels.

Par ailleurs, nous voulons classer les carrés produits en fonction de leur bimagie partielle. Il faut donc pouvoir comparer les carrés entre eux.

Nous devons donc fournir deux méthodes, *equals* et *compareTo*, qui permettent à la structure ensembliste de faire correctement son travail.

Enfin, pour des raisons de performance, nous avons décidé de ne pas pénaliser le thread moteur de génération avec un mécanisme de verrouillage de la structure de données. Nous préférons que le thread utilisateur ait une vue volatile (un *snapshot*) des données qui laisse au thread moteur la possibilité de modifier la structure de donnée pendant la consultation par l'utilisateur.

Pour toutes ces raisons, nous avons opté pour la structure de la librairie Java (1.6) appelée 'ConcurrentSkipListSet'. Elle répond exactement aux besoins ci-dessus décrits.

Chapitre 6

Résultats expérimentaux

Dans le chapitre 4, nous avons calculé le nombre de possibilités pour les différents paramètres intervenants dans la méthode.

Nous avons vu que ce nombre de possibilités devient très vite très grand.

C'est pour cette raison que nous avons décidé, pour l'implémentation, de choisir aléatoirement ces paramètres lors de la génération d'un carré (voir chapitre précédent).

Cependant, comme nous le mentionnions à la fin du chapitre 4, ce grand nombre de possibilités ne veut pas dire qu'il y a autant de carrés magiques générés différents[1]. En effet, plusieurs *jeux* de paramètres différents pourraient conduire au même carré.

Nous nous attaquons dans ce chapitre à une courte étude concernant les carrés générés par notre logiciel.

Nous avons porté notre étude sur l'ordre 7 car le Docteur A. Jacques est intéressé par celui-ci. Comme indiqué dans le chapitre 1, il est vraisemblable qu'il n'existe pas de bimagie pour cet ordre ; mais néanmoins, il peut être intéressant de mesurer la bimagie partielle des carrés générés.

Ce chapitre commence par discuter du nombre de carrés générés différents en fonction de la stratégie de choix de paramètres.

Ensuite, nous nous intéresserons à la répartition de la bimagie partielle des carrés générés.

6.1 Choix des paramètres - Influence sur les carrés générés

Pour obtenir les résultats de la première section, nous avons légèrement modifié notre programme afin qu'il itère systématiquement sur les matrices génératrices et les vecteurs t dans le but de balayer tout l'espace de solutions.

[1] rappelons que nous considérons comme égaux deux carrés qui ont les mêmes valeurs aux mêmes positions

6.1.1 Bijections fixées

Nous choisissons (au hasard) un ensemble de bijections (1 bijection de type c et 2 permutations quelconques). Cet ensemble est fixé et on fait ensuite varier la matrice génératrice X et le vecteur t.

Dans ce cas, le nombre maximum de carrés générés est fixé : c'est le produit du nombre de matrices génératrices différentes et du nombre de vecteurs t différents. Soit :

$$\textit{Nombre de matrices } X \times \textit{Nombre de vecteurs } t = 432 \times 49 = 21\ 168$$

6.1.2 Choix aléatoires de bijections

Cette fois-ci, pour chaque génération, nous allons laisser le logiciel choisir au hasard un ensemble de bijections.

Nous avons procédé à 100 000 générations[2] Nous avons répété chacun de ces tests dix fois.

Pour chacun des test (numerotés de 1 à 10), nous donnons le nombre de doublons générés.

La première ligne donne le numéro du test.

Pour la deuxième, la matrice génératrice X et le vecteur t sont fixés en début d'expérience. A chaque itération, un ensemble de bijections est choisi au hasard.

Dans le troisième ligne, seule la matrice génératrice est fixée.

Dans la quatrième ligne, c'est le vecteur t qui a été fixé.

Dans la dernière ligne, c'est l'ensemble des paramètres (matrices génératrices, bijections et vecteur t) qui varient aléatoirement à chaque itération.

Série de test numéro	1	2	3	4	5	6	7	8	9	10
Matrice X et vecteur t fixés	36	28	23	29	18	23	24	38	23	44
Matrice X fixée	33	23	21	20	26	19	31	34	30	32
Vecteur t fixé	1	2	0	2	2	2	2	2	1	2
Tout aléatoire	2	2	3	1	0	3	3	3	1	4

Nombre de doublons par 100 000 générations.

6.1.3 Analyse des résultats

Rappelons[3] que pour l'ordre 7, il y a plus de 180 000 000 000 000 possibilités de paramètres.

A la vue du tableau ci-dessus, nous constatons que :

1. les taux de doublons sont très petits. Ceci confirme que la méthode peut réellement produire *beaucoup* de carrés magiques différents.

[2] il n'était pas possible, pour cause de dépassement de mémoire, de procéder à plus de tests en une fois.
[3] voir tableau de la fin du chapitre 4

En effet, on constate que, dans les meilleures configurations (les lignes 4 et 5 du tableau), il y a taux de doublons d'environ 2-3 pour 100 000. Ils sont donc quasiment tous différents.

2. on obtient un taux dix fois plus important de doublons quand la matrice génératrice est fixée. Cependant, puisqu'il y a 432 matrices génératrices, l'espace de possibilités est divisé par autant, et il nous semble que le poids relatif de ce paramètre est moins important que celui des bijections.

3. La fixation du vecteur t, par contre, ne semble pas augmenter le taux de doublons. Dès lors, cela nous conduit à dire que ce paramètre n'a (quasi) aucune influence sur le nombre de carrés générés différents.

4. Tous ces résultats devraient être confirmés par des analyses statistiques rigoureuses (écart type, intervalle de confiance, ...)

6.2 Répartition de la bimagie partielle

Dans cette section, nous donnons la répartition des carrés magiques d'ordre 7 en fonction de leur score de bimagie partielle.

Le test a porté sur 1 000 000 d'essais où tous les paramètres étaient choisis aléatoirement à chaque itération.

Bimagie partielle	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Nombre	579107	293800	101879	18299	4874	1206	342	241	173	71	8	0	0	0	0	0	0

Répartition de carrés en fonction de leur bimagie partielle (pour 1 000 000 générations).

On constate que près 58% des carrés générés n'ont aucune bimagie partielle, et près de 98% ont moins de 3 composants de bimagie partielle.

Moins de 1 sur 100 000 possède 10 composants ou plus de bimagie partielle.

Nous ne savons pas si la méthode étudiée peut générer des carrés ayant de meilleurs scores de bimagie partielle.

Cependant, vu le nombre total de possibilités et le faible taux de doublons produits par le logiciel, il reste de la place pour de futures recherches expérimentales avec la méthode.

Chapitre 7

Conclusions

Dans ce travail, nous avons examiné une méthode algébrique qui permet de générer des carrés n-multimagiques.

Nous avons expliqué de manière théorique le fonctionnement de cette méthode et nous l'avons implémenté dans un logiciel.

Cette méthode nous a permis de générer, pour certains des ordres qu'il nous était demandé d'étudier, des carrés magiques, et pour certains autres ordres, des carrés bimagiques.

Les avantages de la méthode sont les suivants :

1. Elle permet de générer un très grand nombre de carrés n-multimagiques (pour les ordres où elle est opérationnelle). Elle offre donc un très grand échantillon de carrés sur lequel il serait alors possible d'effectuer différentes recherches statistiques. Un exemple pourrait être de se demander quelle est la répartition statistique de la bimagie partielle pour un ordre donné. Un autre exemple serait de compter le nombre de carrés hémi-bimagiques trouvés, etc ...

2. L'algorithme qu'elle utilise calcule de manière polynomiale puisqu'il s'agit essentiellement de calculs matriciels.

3. Elle peut être adaptée pour chercher des carrés avec des valeurs particulières pour des indices donnés du carré. Il suffit, pour cela, de résoudre des systèmes d'équations. En effet, il s'agit *grosso modo* d'inverser la matrice génératrice X apparaissant dans la méthode, ce que l'on peut faire puisque celle-ci correspond à un automorphisme.

Néanmoins, nous avons mis en évidence qu'elle présente également quelques inconvénients :

1. Elle ne peut traiter que certains ordres. Entre autres, elle ne peut générer de carrés simplement magiques pour des ordres où il en existe (par exemple, l'ordre 6). Et elle ne génère des carrés bimagiques qu'aux ordres 'carrés parfaits'. D'une manière générale, l'ordre des carrés générés augmente exponentiellement en fonction du degré de multimagie souhaité.

2. Il est difficile de recenser les ensembles de paramètres qui génèrent le même carré. Comme le nombre de possibilités augmente extrêmement vite en fonction de l'ordre du carré, il n'est pas envisageable de les

tester toutes.

L'univers des carrés magiques reste, comme le nôtre, à découvrir pour sa plus grande part. Le présent mémoire ne saurait épuiser le sujet.

Comme développements futurs de cette méthode, nous pensons que les recherches pourraient s'axer dans deux directions :

1. Développer les aspects algébriques afin de pouvoir fixer des valeurs spécifiques pour des positions déterminées du carré.

2. Classer les ensembles de paramètres de la méthode produisant les mêmes carrés.

Pour sa part, le présent travail entendait souligner que dans ces domaines où la combinatoire est très importante, l'apport réciproque d'une théorie mathématique et de la puissance exploratoire de l'outil informatique est essentiel.

Bibliographie

[Descombes 2000] DESCOMBES René
Les Carrés Magiques
Ed. Vuibert, Paris, 2000

[Descombes 2004] DESCOMBES René
La Magie du Carré
Ed. Vuibert, Paris, 2004

[Horstmann 2001] HORSTMANN Cay, CORNELL Gary
Au coeur de Java 2 - Notions Fondamentales Vol 1
Campus Press, Paris, 2001

[Horstmann 2002] HORSTMANN Cay, CORNELL Gary
Au coeur de Java 2 - Notions Avancées Vol 2
Campus Press, Paris, 2002

[Jeanneret 2008] JEANNERET Alain, Lines Daniel
Invitation à l'algèbre - Théorie des groupes, des anneaux, des corps et des modules
Cépadues éditions, Toulouse, 2008

[Jacques, Docteur A. 2008] JACQUES, Docteur Alexandre
Présentation des carrés magiques
correspondance entretenue avec l'auteur, mars 2008

[Leblanc 2007] LEBLANC Jean-Noël
Génération de carrés magiques pour la génétique
Mémoire FUNDP-Institut d'informatique année académique 2006-2007

[Metsker 2006] METSKER Steven John, WAKE William C.
Les Design Patterns en Java
Campus Press, Paris, 2006

[Marco et *al* 2007 Vol1] MARCO Jean-Pierre, LAZZARINI Laurent (sous la direction de)
Mathématiques L1. Cours complet avec 1000 test et exercices corrigés
Ed. Pearson Education France, Paris, 2007

[Marco et *al* 2007 Vol2] MARCO Jean-Pierre, THIEULLEN Philippe, WEIL Jacques-Arthur (sous la direction de)
Mathématiques L2. Cours complet avec 700 test et exercices corrigés
Ed. Pearson Education France, Paris, 2007

[Monnier 2003] MONNIER Jean-Marie
Algèbre MPSI - Cours et 700 exercices corrigés
Dunod 3^{me} édition, Paris, 2003

[Multimagic Squares 2005] DERKSEM Harm, EGGERMONT Christian, van den ESSEN Arno
Multimagic Squares
http ://arXiv :math/0504083v2, April 2005 - annexé au présent travail.

[Site Morgenstern] http ://home.earthlink.net/ morgenstern/magic/biproof.htm
[Site Multimagie] http ://www.multimagie.com/
[Site Trump] http ://www.trump.de/magic-squares/estimates/multi.htm
[Small Rings] http ://www.mathe2.uni-bayreuth.de/axel/htmlpapers/noebauer/html

Annexe

Multimagic Squares

Harm Derksen, Christian Eggermont, Arno van den Essen

February 1, 2008

Abstract

In this paper we give the first method for constructing n-multimagic squares (and hypercubes) for any n. We give an explicit formula in the case of squares and an effective existence proof in the higher dimensional case. Finally we prove that n-multimagic squares do not exist for certain orders.

Introduction

Magic squares have been studied over 4000 years. Recently some exciting new results have been found considering these squares. For instance the first method of constructing all most-perfect magic squares and their enumeration appeared in [3] (See also [14]). Also the non-existence of a 8×8 magic knights tour ([13]) has been verified by computers. Finally a very natural connection has been found between the properties and construction of Franklin's squares and his magic circles ([10]). However, there are still many unsolved problems (e.g. [1], [12]) and as Clifford Pickover says *"the field of magic square study is wide open"* ([12], p. 26). In this paper we will concentrate on so called multimagic squares.

Suppose that M is an $m \times m$ matrix M consisting of natural numbers. Then M is called a magic square if the sum of all elements in each column, row and main diagonal gives the same number; the so-called magic number. Let M^{*d} be the matrix obtained by raising each element of M to the d-th power. The matrix M is called an n-multimagic square (where n is a fixed positive natural number) if M^{*d} is a magic square for $d = 1, 2, \ldots, n$. The matrix M is called normal if its matrix elements consist of the consecutive integers $1, 2, \ldots, m^2$. Throughout this paper we always consider normal magic squares (of course if $m > 1$ and $d > 1$ then the matrix M^{*d} is not normal).

The first 2-multimagic square was published by Pfeffermann in 1891: it has order 8 (Figure 1, [11], [5]). In 1905 the first 3-multimagic square was constructed by Tarry: it has order 128. In 2001 both a 4- and a 5-multimagic square were constructed by Boyer and Viricel respectively of order 512 and 1024 ([4], [5] where they also give a nice history on the subject). The record up to now was a 6-multimagic square of order 4096 constructed by Pan Fengchu in October 2003 ([8]).

56	34	8	57	18	47	9	31
33	20	54	48	7	29	59	10
26	43	13	23	64	38	4	49
19	5	35	30	53	12	46	60
15	25	63	2	41	24	50	40
6	55	17	11	36	58	32	45
61	16	42	52	27	1	39	22
44	62	28	37	14	51	21	3

Figure 1: G. Pfeffermann, 1891

In this paper we give a constructive procedure to make a large class of n-multimagic squares for each positive integer $n \geq 2$. The problem of finding such squares is reduced to an easy linear algebra problem which is solved in general in section 4. A more explicit solution is described in section 3. This solution is used to give an explicit formula for n-multimagic squares for all $n \geq 3$. In particular it gives the first 7-multimagic squares, of order 13^7 and 8-multimagic squares of order 17^8 etc.

The method described for constructing n-multimagic squares can easily be extended to n-multimagic cubes and hypercubes. We refer to section 4 for all definitions and more details.

1 Preliminaries

Throughout this paper R denotes a finite ring with q elements. Let $R^\star$ denote the set of elements in R which have a multiplicative inverse.

Definition 1.1 *For $c \in R$ we call a bijection $N : R \to \{0, 1, \ldots, q-1\}$ of type c if $N(a) + N(-a + c) = q - 1$ for all $a \in R$.*

Lemma 1.2

i). If $2 \in R^\star$, then for every $c \in R$ there exists a bijection N of type c.

ii). If $2 \notin R^\star$, then for every $c \in R^\star$ there exists a bijection N of type c.

Proof. For $c \in R$ define $\varphi = \varphi_c : R \to R$ by $\varphi(a) = -a + c$ for all $a \in R$. Then φ^2 is equal to the identity. So all orbits of φ have length 1 or 2. An element a is a fixed point of φ if and only if $2a = c$. For $a \in R$ denote its orbit under φ by $O(a)$.
i) Let 2 be a unit in R. Then φ has exactly one fixed point, namely $a_0 := 2^{-1}c$. The orbit $O(a_0)$ of a_0 has one element. Let $O(a_1), O(a_2), \ldots, O(a_s)$ be the other orbits. They all have two elements. In particular, we get $s = (q-1)/2$. Define $N(a_0) = s$, $N(a_i) = i - 1$ and $N(\varphi(a_i)) = q - 1 - N(a_i)$ $(= q - i)$, for $i = 1, 2, \ldots, s$. Now N is as desired.
ii) Let 2 not be a unit in R. Then for $c \in R^\star$, $\varphi = \varphi_c$ has no fixed points. Indeed, if

$\varphi(a) = a$, then we get $2a = c \in R^\star$. So $2 \in R^\star$ and we have a contradiction. We can write $R = \bigcup_{i=1}^{s} O(a_i)$, where each $O(a_i)$ is an orbit with two elements. In particular, $s = q/2$. Define $N(a_i) = i - 1$ and $N(\varphi(a_i)) = q - 1 - N(a_i)$ $(= q - i)$ for all i. Then N is as desired. □

Let m be a positive integer. For each $1 \leq j \leq m$ we choose a bijection

$$N_{(j)} : R \to \{0, 1, \ldots, q-1\}$$

of type c_j, for some $c_j \in R$ (this is possible by Lemma 1.2). Put $c = (c_1, \ldots, c_m) \in R^m$ and define $N_m : R^m \to \{1, 2, \ldots, q^m\}$ by

$$N_m(a_1, \ldots, a_m) = 1 + \sum_{j=1}^{m} q^{j-1} N_{(j)}(a_j).$$

Since the coefficients of the q-adic expansion of any natural number are unique and each $N_{(j)}$ is a bijection, it follows that N_m is a bijection.

Lemma 1.3 *$N_m(-a) = q^m + 1 - N_m(a + c)$, for all $a = (a_1, \ldots, a_m) \in R^m$.*

Proof. From definition 1.1 follows that

$$N_m(-a) + N_m(a + c) = 2 + \sum_{j=1}^{m} q^{j-1}(N_{(j)}(-a_j) + N_{(j)}(a_j + c_j)) =$$

$$= 2 + (1 + q + \ldots + q^{m-1})(q - 1) = 2 + (q^m - 1) = q^m + 1.$$

□

To conclude this section we will give a result (proposition 1.5) which plays a crucial role in the next section. First some notations. Let n and s be positive integers. Suppose that $L : R^n \to R^s$ is an affine map, i.e., there exists an R-module homomorphism $L_0 : R^n \to R^s$ and a vector $v \in R^s$ such that

$$L(a) = L_0(a) + v, \quad a \in R^n.$$

Lemma 1.4 *If $L : R^n \to R^s$ is a surjective affine map, then $\#L^{-1}(y) = q^{n-s}$ for all $y \in R^s$.*

Proof. Let $y \in R^s$. Since L is surjective there exists $a_0 \in R^n$ such that $L(a_0) = y$. It follows that $L^{-1}(y) = a_0 + \ker L_0$. Since L is surjective, so is L_0. It follows that $R^n / \ker L_0 \simeq R^s$, whence $\#\ker L_0 = q^{n-s}$ and consequently $\#L^{-1}(y) = q^{n-s}$. □

Proposition 1.5 *Suppose that $L : R^n \to R^s$ is a surjective affine map. For each $j \in \{1, 2, \ldots, s\}$, let $N_{(j)} : R \to \{0, 1, \ldots, q-1\}$ be a bijection. For any nonnegative integers $e_1, \ldots, e_s$ we have*

$$\sum_{a \in R^n} N_{(1)}(L(a)_1)^{e_1} \ldots N_{(s)}(L(a)_s)^{e_s} = q^{n-s} \left(\sum_{i=0}^{q-1} i^{e_1} \right) \ldots \left(\sum_{i=0}^{q-1} i^{e_s} \right).$$

Proof. Let $y = (y_1, \ldots, y_s) \in R^s$. Then for each $a \in L^{-1}(y)$ we get

$$N_{(1)}(L(a)_1)^{e_1} \ldots N_{(s)}(L(a)_s)^{e_s} = N_{(1)}(y_1)^{e_1} \ldots N_{(s)}(y_s)^{e_s}.$$

So by Lemma 1.4 we obtain

$$\sum_{a \in L^{-1}(y)} N_{(1)}(L(a)_1)^{e_1} \ldots N_{(s)}(L(a)_s)^{e_s} = q^{n-s} N_{(1)}(y_1)^{e_1} \ldots N_{(s)}(y_s)^{e_s}. \tag{1}$$

Since L is surjective, R^n is the disjoint union of the fibres $L^{-1}(y)$, $y \in R^s$. We deduce from (1) that

$$\begin{aligned}
&\sum_{a \in R^n} N_{(1)}(L(a)_1)^{e_1} \ldots N_{(s)}(L(a)_s)^{e_s} \\
&= \sum_{y \in R^s} \sum_{a \in L^{-1}(y)} N_{(1)}(L(a)_1)^{e_1} \ldots N_{(s)}(L(a)_s)^{e_s} \\
&= \sum_{y \in R^s} q^{n-s} N_{(1)}(y_1)^{e_1} \ldots N_{(s)}(y_s)^{e_s} \\
&= q^{n-s} \left(\sum_{y_1 \in R} N_{(1)}(y_1)^{e_1} \right) \ldots \left(\sum_{y_s \in R} N_{(s)}(y_s)^{e_s} \right).
\end{aligned}$$

Since each $N_{(j)} : R \to \{0, 1, \ldots, q-1\}$ is a bijection we get that

$$\sum_{y_j \in R} N_{(j)}(y_j)^{e_j} = \sum_{i=0}^{q-1} i^{e_j},$$

which concludes the proof. □

2 A construction of n-multimagic squares

Let $n \in \mathbb{N}$. The following theorem gives the main tool for constructing n-multimagic squares. We will use the notations introduced in the previous section. Let R be a finite ring with q elements. Write $Gl_m(R)$ for the ring of $m \times m$ invertable matrices over R.

First we choose $c_1, \ldots, c_n$ in R and n bijections

$$N_{(1)}, \ldots, N_{(n)} : R \to \{0, 1, \ldots, q-1\}$$

of types $c_1, \ldots, c_n$ respectively. With these (not necessarily different) bijections we define

$$N_n : R^n \to \{1, 2, \ldots, q^n\}$$

as described in section 1. This choice will be fixed throughout this section. In a similar way we fix a bijection

$$N'_{2n} : R^{2n} \to \{1, 2, \ldots, q^{2n}\}$$

using bijections $N'_{(1)}, \ldots, N'_{(2n)}$ of type $c'_1, \ldots, c'_{2n}$ respectively.

Definition 2.1 *A matrix $X \in Gl_{2n}(R)$ is called an n-multimagic generator matrix if for the matrices $A, B \in \mathrm{Mat}_{2n,n}(R)$ such that $X = (A\ B)$, all $n \times n$ minors of $A, B, A + B$ and $A - B$ are units in R.*

Theorem 2.2 *Suppose that $X \in Gl_{2n}(R)$ is an n-multimagic generator matrix. For any $t \in R^{2n}$ the $q^n \times q^n$ matrix M defined by*

$$M_{N_n(a),N_n(b)} = N'_{2n}\left(X\begin{pmatrix} a \\ b \end{pmatrix} + t\right), \quad a, b \in R^n$$

is n-multimagic.

Note that the matrix M in the theorem is well-defined because $N_n(a)$ takes each value in $\{1, 2, \ldots, q^2\}$ exactly once, and so does $N_n(b)$.

Proof.
i) First observe that all matrix elements M_{ij} are distinct since $X \in Gl_{2n}(R)$ and N'_{2n} is a bijection. Consequently the matrix M consists exactly of all elements of the set $\{1, 2, \ldots, q^{2n}\}$, so M is normal.
ii) Now let d be an integer with $1 \leq d \leq n$ and write $X = (A\ B)$ with $A, B \in \mathrm{Mat}_{2n,n}(R)$. First we want to show that the sum of all elements in any column of M^{*d} is the same constant which only depends on q and n. Fix $b \in R^n$. Then the $N_n(b)$-th column of M^{*d} consists of the elements $M^d_{N_n(a),N_n(b)}$, where a runs through R^n (remember that $N_n : R^n \to \{1, 2, \ldots, q^n\}$ is a bijection).
Let $S_b(d)$ be the sum of the elements of the $N_n(b)$-th column of M^{*d}, so

$$S_b(d) = \sum_{a \in R^n} M^d_{N_n(a),N_n(b)}.$$

To compute $S_b(d)$ first observe that the j-th component of the vector $X\binom{a}{b} = (A\ B)\binom{a}{b}$ is equal to $A_{(j)} \cdot a + B_{(j)} \cdot b$, where $A_{(j)}$ (respectively $B_{(j)}$) denotes the j-th row of A (respectively B). Using the definitions of $M_{N_n(a),N_n(b)}$ and N'_{2n} we get

$$S_b(d) = \sum_{a \in R^n} \left(1 + \sum_{j=1}^{2n} C_j(a, b)\right)^d \tag{2}$$

where

$$C_j(a,b) = q^{j-1}N'_{(j)}(A_{(j)}.a + B_{(j)}.b + t_j), \text{ for all } 1 \leq j \leq 2n. \tag{3}$$

Now observe that $(1+x_1+\cdots+x_{2n})^d$ can be written as $1+g$, where g is a sum of terms of the form $\alpha x_{j_1}^{e_1}\ldots x_{j_s}^{e_s}$, where $1 \leq j_1 < j_2 \ldots < j_s \leq 2n$, $e_1,\ldots,e_s \geq 1$ and $e_1+\cdots+e_s \leq d$ (so in particular $s \leq d \leq n$) and α is a positive integer. So it follows from (2) that $S_b(d)$ only depends on q and n if we can show that for each set of exponents $e_1,\ldots,e_s$ and indices $j_1,\ldots,j_s$ as above, the sum

$$\sum_{a\in R^n} C_{j_1}(a,b)^{e_1}\ldots C_{j_s}(a,b)^{e_s} \tag{4}$$

only depends on q and n (and of course $e_1,\ldots,e_s$, $j_1,\ldots,j_s$). To see this we are going to use Proposition 1.5. Therefore put $J = (j_1,\ldots,j_s)$ and define the affine map $L : R^n \to R^s$ by the formula

$$L(a) = A_{(J)} \cdot a + B_{(J)} \cdot b + t_J$$

where $A_{(J)}$ (respectively $B_{(J)}$) is the $s \times n$ matrix with rows $A_{(j_1)},\ldots,A_{(j_s)}$ (respectively $B_{(j_1)},\ldots,B_{(j_s)}$) and $t_{(J)}$ in the column of length s with components $t_{j_1},\ldots t_{j_s}$. Since, as observed above, $s \leq n$ and all $n \times n$ minors of A are units in R (by hypothesis) it follows that $L : R^n \to R^s$ is surjective. By (3) we have $C_{j_i}(a,b) = q^{j_i-1}N'_{(j_i)}(L(a)_i)$ for all $1 \leq i \leq s$. It follows from Proposition 1.5 that the expression in (4) is equal to

$$q^{n-s} \cdot q^{e_1(j_1-1)+\cdots+e_s(j_s-1)} \cdot \left(\sum_{i=0}^{q-1} i^{e_i}\right)\ldots\left(\sum_{i=0}^{q-1} i^{e_s}\right) \tag{5}$$

which indeed only depends on q and n, as desired.

iii) Interchanging the roles of a and b in the argument given in ii) we get that all rowsums of M^{*d} are equal to the same constant.

iv) Now let us compute the sum of the (main) diagonal elements of M^{*d}. This sum is equal to

$$D(d) = \sum_{a\in R^n} M^d_{N_n(a),N_n(a)}.$$

To compute $D(d)$ we just repeat the arguments given in ii) with $b = a$. It then remains to show that the expression in (4) with $b = a$ equals the expression given in (5), since this results in $D(d)$ being equal to the same constant as the rows. Therefore just observe that $C_{j_i}(a,a) = q^{j_i-1}N'_{(j_i)}(L_1(a)_i)$ for all $1 \leq i \leq s$, where $L_1 : R^n \to R^s$ is the affine map defined by

$$L(a) = A_{(J)} \cdot a + B_{(J)} \cdot a + t_{(J)} = (A+B)_{(J)} \cdot a + t_{(J)}$$

(recall that $J = (j_1,\ldots,j_s)$). Since by hypothesis all $n \times n$ minors of $A+B$ are units in R, it follows that L is surjective. Then using Proposition 1.5 again we obtain that the expression in (4) with $b = a$ is indeed equal to the expression given in (5).

v) Finally we compute the sum of all elements from the "second" diagonal of M^{*d}. This sum $D'(d)$ is equal to

$$D'(d) = \sum_{a \in R^n} M^d_{N_n(a), q^n+1-N_n(a)}.$$

Since by lemma 1.3 $q^n + 1 - N_n(a) = N_n(-a + c)$ we get

$$D'(d) = \sum_{a \in R^n} M^d_{N_n(a), N_n(-a+c)}.$$

Then repeating the arguments in ii) with b replaced by $-a + c$ leads us to define the affine map $L' : R^n \to R^s$ by

$$L'(a) = A_{(J)} \cdot a + B_{(J)}(-a + c) + t_{(J)} = (A - B)_{(J)} \cdot a + (B_{(J)} \cdot c + t_{(J)}).$$

The map L' is surjective since all $n \times n$ minors of $A - B$ are units in R. So again we find that the expression in (4) with b replaced by $-a + c$ is equal to the expression in (5), resulting in $D'(d)$ being equal to the same constant, which completes the proof of this theorem. □

3 Finding Generator Matrices

In order to be able to construct effectively n-multimagic squares by the method described in theorem 2.2, we need to show how to find a ring R and a n-multimagic generator matrix $X \in Gl_{2n}(R)$ which satisfy the conditions of that theorem.

Below we describe an explicit construction of (n-multimagic) generator matrices. For an effective existence proof in a more general setting see section 4.2.

Lemma 3.1 *Let $n \geq 1$ and R a ring such that 2 and 3 are units in R. If A is an $2n \times n$ matrix such that every $n \times n$ minor of A is a unit in R, then there exists an $2n \times n$ matrix B such that $(A\ B)$ is an n-multimagic generator matrix. More precisely, if $A = \binom{P}{Q}$ with $P, Q \in \mathrm{Mat}_{n,n}(R)$, then we can take $B = \binom{2P}{-2Q}$.*

Proof. Since 2 is a unit in R the hypothesis on P and Q implies that also the $n \times n$ minors of B are units in R. Furthermore the $n \times n$ minors of $A + B = \binom{3P}{-Q}$ are also units in R, since 3 and -1 are. Similarly the $n \times n$ minors of $A - B$ are units in R. Finally, using elementary column operators one can reduce the matrix $(A\ B) = \binom{P\ \ 2P}{Q\ -2Q}$ to the matrix $\binom{P\ \ 0}{Q\ -4Q}$ which is clearly invertible over R since both $\det P$ and $\det(-4Q)$ are units in R. □

Lemma 3.2 *Let $n \geq 2$ and define the $2n \times n$ matrix A by $A_{i,j} = (i-1)^{j-1}$ for $i = 1, 2, \ldots, 2n-1$ and $j = 1, 2, \ldots, n$ ($0^0 = 1$), $A_{2n,j} = 0$ for $j = 1, 2, \ldots, 2n-1$ and*

$A_{2n,n} = 1$. *So we have*

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 4 & \cdots & 2^{n-1} \\ 1 & 3 & 9 & \cdots & 3^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & (2n-2) & (2n-2)^2 & \cdots & (2n-2)^{n-1} \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

If R is a ring then we may view A as a matrix with entries in R. If $\{1, 2, \ldots, 2n-2\} \subseteq R^\star$, then all $n \times n$ minors of A are units in R.

Proof. Using Vandermonde determinants one easily verifies that each factor appearing in each $n \times n$ minor of A is of the form $i - j$ where $0 \leq j < i \leq 2n-2$, from which the desired result follows. □

As an immediate consequence of the lemmas above we get

Corollary 3.3 *Let $n \geq 2$ and R be a ring such that $\{3, 1, 2, \ldots, 2n-2\} \subseteq R^\star$, then the matrix $(A\ B)$ is an n-multimagic generator matrix where A is as in Lemma 3.2 and B is as in Lemma 3.1.*

In theorem 3.4 below we choose one bijection $N : R \to \{0, 1, \ldots, q-1\}$ of some type $c \in R$ and define for each $m \geq 1$

$$N_m(a_1, \ldots, a_m) = 1 + \sum_{j=1}^{m} q^{j-1} N(a_j).$$

So in the definition of N_m as given in section 1 we take all $N_{(j)}$ to be equal to N.

Theorem 3.4 *(An explicit formula for n-multimagic squares.)*
Let $n \geq 3$, q a prime number $\geq 2n-1$, $R = \mathbb{F}_q$ and $N : R \to \{0, 1, \ldots, q-1\}$ the bijection (of type -1) given by $N(\bar{i}) = i$ for all $0 \leq i \leq q-1$. Let A and B be as in 3.3. Then for $X = (A\ B)$ and each $t \in R^{2n}$ the matrix M defined in 2.2 is n-multimagic.

In other words, for every positive integer n there exists a (normal) n-multimagic square. In particular for $n = 7$ we get 7-multimagic squares of orders 13^7, 17^7, 19^7 etcetera. For $n = 8$ we get 8-multimagic squares of orders 17^8, 19^8, 23^8 etcetera.

4 Multimagic cubes and hypercubes

In this section we briefly indicate how the method developed in the previous sections can be extended to construct multimagic cubes, perfect multimagic cubes and hypercubes.

4.1 Multimagic cubes

Note that there is no consensus on the definition of multimagic cubes (hypercubes etc.) in the literature. The choice given below can also be found in [15], [9].

A cube of numbers (respectively the consecutive numbers $1, 2, \ldots, n^3$) is called magic (respectively normal magic) if the sum of all elements in each row, column and pillar is the same and is equal to the sum of all elements of each of the four space diagonals. Furthermore, if $n \geq 1$ such a cube is called n-multimagic if for each $1 \leq d \leq n$ the cube obtained by raising each of its elements to the d-th power is magic.

Completely analogues to the construction of n-multimagic squares in 2.2 we define a $q^n \times q^n \times q^n$ cube by the formula

$$M_{N_n(a),N_n(b),N_n(c)} = N'_{3n}\left((A\ B\ C)\begin{pmatrix} a \\ b \\ c \end{pmatrix} + t\right)$$

where each of the vectors a, b and c runs through R^n, $t \in R^{3n}$ and A, B and C are matrices in $\mathrm{Mat}_{3n,n}(R)$ which satisfy the following properties (which guarantee the matrix M to be an n-multimagic cube):

1. $(A\ B\ C) \in Gl_{3n}(R)$ (which guarantees that all the natural number $1, 2, \ldots, q^{3n} (= (q^n)^3)$ appear in M).
2. all $n \times n$ minors of the matrices A, B and C are units in R (which guarantees that for each $1 \leq d \leq n$ the sum of all elements in each column, row and pillar of M^{*d} is the same, and hence equal to the magic sum).
3. all $n \times n$ minors of the matrices $A+B+C$, $-A+B+C$, $A-B+C$ and $A+B-C$ are units in R (which guarantees that for each $1 \leq d \leq n$ the sum of all elements on each of the four space diagonals of M^{*d} is equal to the magic sum).

Recall that a magic cube is called perfect if additionally the diagonals of each orthogonal slice have the magic sum property. Furthermore, if $n \geq 1$ such a cube is called n-multimagic perfect if for each $1 \leq d \leq n$ the cube obtained by raising each of its elements to the d-th power is perfect magic.

To guarantee that a n-multimagic cube M as above is also n-multimagic perfect we impose on the matrices A, B, C the following conditions

4. all $n \times n$ minors of the matrices $A + B$, $A - B$, $A + C$, $A - C$, $B + C$ and $B - C$ are units in R.

4.2 More Generator Matrices

To find a ring R and matrices A, B and C satisfying the properties 1, 2, 3 and 4 one can use the method described below. To facilitate generalizations to (even) higher dimensions we give a more general notion of generator matrix:

Definition 4.1 *Let d be a positive integer ≥ 2. We call a matrix $X \in Gl_{dn}(R)$ an n-multimagic d-generator matrix if when we write $X = (A_1 \ \ldots \ A_d)$ with $A_1, \ldots, A_d \in \mathrm{Mat}_{dn,n}(R)$, we have that for $\delta_1, \ldots, \delta_d \in \{-1, 0, 1\}$ not all 0, the matrix*

$$\sum_{i=1}^{d} \delta_i A_i$$

has all $n \times n$ minors in $R^\star$.

Note that the four properties of the matrix $(A\ B\ C)$ of the previous section are equivalent to saying that it is a n-multimagic 3-generator matrix.

Example 4.2 A 1-multimagic 3-generator matrix with $R = \mathbb{F}_q$ with q prime and $q \geq 11$:

$$\begin{pmatrix} 1 & 2 & 4 \\ 1 & 2 & -4 \\ 1 & -2 & -4 \end{pmatrix}$$

Example 4.3 A 2-multimagic 3-generator matrix with $R = \mathbb{F}_q$ with q prime and $q \geq 11$:

$$\begin{pmatrix} 1 & 0 & 2 & 0 & 4 & 0 \\ 1 & 1 & 2 & 2 & 4 & 4 \\ 1 & 2 & 2 & 4 & -4 & -8 \\ 1 & 3 & 2 & 6 & -4 & -12 \\ 1 & 4 & -2 & -8 & -4 & -16 \\ 0 & 1 & 0 & -2 & 0 & -4 \end{pmatrix}$$

Example 4.4 A 2-multimagic 2-generator matrix with $R = \mathbb{F}_q$ with q prime and $q \geq 11$, $q \neq 17$:

$$\begin{pmatrix} 1 & 0 & 0 & -1 & -2 & -1 \\ 0 & 1 & 0 & -1 & -1 & -2 \\ 0 & 0 & 1 & -2 & -1 & -1 \\ 1 & 2 & 1 & 1 & 0 & 0 \\ 1 & 1 & 2 & 0 & 1 & 0 \\ 2 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The following (well-known) lemma is the crucial tool in finding effectively d-generator matrices for all d.

Lemma 4.5 *Let $m \geq 1$ and $Q(x_1, \ldots, x_m)$ a non-zero polynomial in the variables $x_1, \ldots, x_m$ over $\mathbb{Z}$. Then one can effectively find integers $a_1, \ldots, a_m$ such that $Q(a_1, \ldots, a_m) \neq 0$.*

Proof. We will use induction on m. The case $m = 1$ is obvious since $Q(x_1)$ has at most $\deg Q$ zeros. Now let $m \geq 2$. Write $Q = q_d(x_1, \ldots, x_{n-1})x_m^d + \cdots + q_1(x_1, \ldots, x_{m-1})x_m + q_0(x_1, \ldots, x_{m-1})$ with $q_d \neq 0$. By the induction hypothesis there exist integers $a_1, \ldots, a_{m-1}$

such that $q_d(a_1, \ldots, a_{m-1}) \neq 0$. So the polynomial $q(x_m) = Q(a_1, \ldots, a_{m-1}, x_m)$ in $\mathbb{Z}[x_m]$ is non-zero and has x_m-degree d. Consequently there exists an integer a_m such that

$$q(a_m) = Q(a_1, \ldots, a_{m-1}, a_m) \neq 0,$$

as desired. □

Proposition 4.6 *Let $n \geq 1$ and $d \geq 2$. Then one can effectively find a positive integer $q > 1$ and matrices $A_1, \ldots, A_d \in \mathrm{Mat}_{dn,n}(\mathbb{Z}/q\mathbb{Z})$ such that $X = (A_1 \ \ldots \ A_d) \in Gl_{dn}(\mathbb{Z}/q\mathbb{Z})$ is an n-multimagic d-generator matrix.*

Proof. To avoid complicating an easy matter we only give a proof for $d = 2$. For other d the procedure is similar.
Let $A_u = (A_{i,j})$ and $B_u = (B_{i,j})$ be two universal $2n \times n$ matrices, i.e., the entries $A_{i,j}$ and $B_{i,j}$ are distinct variables. Then each $n \times n$ minor of A_u, B_u, $A_u + B_u$ and $A_u - B_u$ is a non-zero polynomial in the $4n^2$-variable polynomial ring $\mathbb{Z}[A_{ij}, B_{ij}, 1 \leq i \leq 2n, 1 \leq j \leq n]$. Let P be the product of all these minors and let Q be the product of P and the polynomial $\det(A_u \ B_u)$. By lemma 4.5 we can find integers $a_{i,j}$ and $b_{i,j}$ such that $Q(a_{i,j}, b_{i,j})$ is a non-zero integer. Finally let q be a positive integer > 1 such that $\gcd(Q(a_{i,j}, b_{i,j}), q) = 1$ for all i, j. Then one easily verifies that $X = (a_{ij})$ and $B = (b_{ij})$ represent matrices in $\mathrm{Mat}_{2n,n}(\mathbb{Z}/q\mathbb{Z})$ having the desired properties. □

4.3 Perfect Multimagic Hypercubes

From the above it is now clear how to generalize these definitions and constructions to higher dimensional hypercubes.

Theorem 4.7 *For all integers $d \geq 2$ and $n \geq 1$ there exists a normal perfect n-multimagic d-dimensional hypercube.*

5 Orders

We take a short look at the possible orders a n-multimagic square might have. First we will show that we can use n-multimagic squares to construct new n-multimagic squares of different orders.

Definition 5.1 *Let $A \in \mathrm{Mat}_{m,m}(R)$ and $B \in \mathrm{Mat}_{n,n}(R)$. We define $A \star B \in \mathrm{Mat}_{mn,mn}(R)$ by*

$$A \star B_{mk+i,ml+j} = m^2 B_{k,l} + A_{i,j}$$

where $0 \leq i, j \leq m-1$ and $0 \leq k, l \leq n-1$.

Proposition 5.2 *If $A \in \mathrm{Mat}_{m,m}(R)$ and $B \in \mathrm{Mat}_{n,n}(R)$ are p-multimagic squares then $A \star B$ is an p-multimagic square.*

Proof. The proof is a straightforward calculation so we only explicitly show that the columnsum is independent of the columnindex. We use the same notations as in the definition above. Fix $1 \leq e \leq p$. We denote $S_x = \sum_i A^x_{i,j}$ and $T_x = \sum_i B^x_{i,j}$ for $1 \leq x \leq p$. Since A and B are p-multimagic squares these S_x and T_x are constants. Fix the columnindex $\beta = ml + j$ and write $\alpha = mk + i$.

$$\begin{aligned}
\sum_{\alpha=0}^{mn-1} (A \star B)^e_{\alpha,\beta} &= \sum_{k=0}^{m-1}\sum_{i=0}^{n-1} \left(m^2 B_{k,l} + A_{i,j}\right)^e \\
&= \sum_k \sum_i \sum_{x=0}^{e} \binom{e}{x} \left(m^2 B_{k,l}\right)^{e-x} A^x_{i,j} = \sum_k \sum_x \binom{e}{x} m^{2(e-x)} B^{e-x}_{k,l} \sum_i A^x_{i,j} \\
&= \sum_k \sum_x \binom{e}{x} m^{2(e-x)} S_x B^{e-x}_{k,l} = \sum_x \binom{e}{x} m^{2(e-x)} S_x \sum_k B^{e-x}_{k,l} \\
&= \sum_x \binom{e}{x} m^{2(e-x)} S_x T_{e-x}
\end{aligned}$$

So the columnsum is independent of β, hence a constant. □

From the foregoing one might get the impression that n-multimagic squares are constructable for all (large enough) orders. This is not the case as we will prove next.

Definition 5.3 *If p is a prime and n is a positive integer, then we define $v_p(n)$ as the largest nonnegative integer e such that p^e divides n. For a non-zero rational number $\frac{n}{m}$ we define $v_p(\frac{n}{m}) = v_p(n) - v_p(m)$.*

Lemma 5.4 *(basic properties of v_p)*
Let $a, e, m, p \in \mathbb{N}$ with p prime.

i) $v_p(r \cdot s) = v_p(r) + v_p(s)$ for any non-zero rational numbers r and s

ii) If $v_p(m) = e$ and $1 \leq a \leq p^e$ then $v_p(m^2 - a) = v_p(a)$.

Proof. Straightforward using the unique factorization of integers. □

Theorem 5.5 *Let M be a normal n-multimagic square of order m and $p \in \mathbb{N}$ a prime. If $v_p(m) = e \geq 1$ then $n \leq p^{e+1} - 2$.*

Proof. Write $M = (m_{i,j})_{i,j=1..m}$. Note that if $f \in \mathbb{C}[x]$, $f(\mathbb{Z}) \subseteq \mathbb{Z}$ and $deg_x(f) \leq n$ then the matrix $M^{\circ f} = (f(m_{i,j}))_{i,j=1..m} \in \mathrm{Mat}_{m,m}(\mathbb{Z})$ is also a (general) magic square. Take $f(x) = \binom{x-1}{n} \in \mathbb{Q}[x]$ and note that it is a polynomial of degree n with $f(\mathbb{Z}) \subseteq \mathbb{Z}$. Since $M^{\circ f}$ is magic the sum of all m^2 elements of $M^{\circ f}$ is an integer which is m times

the magic sum, i.e. the sum of any row or column. Since $f(\mathbb{Z}) \subseteq \mathbb{Z}$ the magic sum is an integer which implies that m divides

$$\sum_{x=1}^{m^2} f(x) = \sum_{x=1}^{m^2} \binom{x-1}{n} = \binom{m^2}{n+1}.$$

This means that the (rational) number

$$\frac{m(m^2-1)(m^2-2)\cdots(m^2-n)}{(n+1)!} \tag{6}$$

is really an integer.
Since an n-multimagic square of order m can not exist if an $(n-1)$-multimagic square of order m does not exist, it is enough to show that the case $n = p^{e+1} - 1$ is impossible by showing that (6) is not an integer.
So assume $n = p^{e+1} - 1$. Note that (6) is not equal to 0 since p^e divides m, so in particular $m^2 \geq p^{2e} > p^{e+1} - 1 = n$ (remember e is positive). Using lemma 5.4 we see that

$$\begin{aligned}
v_p\left(\frac{m(m^2-1)(m^2-2)\cdots(m^2-n)}{(n+1)!}\right) &= \\
v_p\left(\frac{m}{n+1}\cdot\frac{(m^2-1)}{1}\cdot\frac{(m^2-2)}{2}\cdots\frac{(m^2-n)}{n}\right) &= && \text{(use lemma 5.4 i))} \\
v_p\left(\frac{m}{n+1}\right) + \sum_{i=1}^{n} v_p\left(\frac{m^2-i}{i}\right) &= && \text{(use lemma 5.4 ii))} \\
v_p\left(\frac{m}{n+1}\right) + \sum_{i=1}^{n} 0 &= \\
v_p\left(\frac{m}{p^{e+1}}\right) &= \\
e-(e+1) &= -1
\end{aligned}$$

So (6) is not a integer if $n = p^{e+1} - 1$. □

In particular this shows that there are no 3-multimagic squares of order $m \equiv 2 \pmod 4$.

6 More Examples

To conclude this paper we give some interesting multimagic squares using theorem 2.2.

In 6.1 - 6.3 below we choose one bijection $N : R \to \{0, 1, \ldots, q-1\}$ of some type $c \in R$ and define for each $m \geq 1$

$$N_m(a_1, \ldots, a_m) = 1 + \sum_{j=1}^{m} q^{j-1} N(a_j).$$

So in the definition of N_m as given in section 1 we take all $N_{(j)}$ to be equal to N. The notations are as in theorem 2.2, where we take $N'_{2n} = N_{2n}$.

Example 6.1 (A family of associative bimagic squares of order 16.)
Take $R = \mathbb{F}_2[x]/(x^2 + x + 1)$,

$$X = \begin{pmatrix} x & 0 & 1 & x \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ x & 1 & 0 & x \end{pmatrix},$$

$t \in R^4$ arbitrary and $N : R \to \{0, 1, 2, 3\}$ (a bijection of type $x + 1$) given by $N(0) = 0$, $N(1) = 2$, $N(x) = 1$ and $N(x + 1) = 3$.
Then the corresponding matrix M defined in theorem 2.2 is bimagic (= 2-multimagic) and associative (= the sum of any pair of matrix elements which are symmetric with respect to the center of the square is equal to $16^2 + 1$).

41	252	74	155	125	176	30	207	129	84	226	51	213	8	182	103
62	239	93	144	106	187	9	220	150	71	245	40	194	19	161	116
3	210	100	177	87	134	56	229	171	122	204	25	255	46	160	77
24	197	119	166	68	145	35	242	192	109	223	14	236	57	139	90
240	61	143	94	188	105	219	10	72	149	39	246	20	193	115	162
251	42	156	73	175	126	208	29	83	130	52	225	7	214	104	181
198	23	165	120	146	67	241	36	110	191	13	224	58	235	89	140
209	4	178	99	133	88	230	55	121	172	26	203	45	256	78	159
98	179	1	212	54	231	85	136	202	27	169	124	158	79	253	48
117	168	22	199	33	244	66	147	221	16	190	111	137	92	234	59
76	153	43	250	32	205	127	174	228	49	131	82	184	101	215	6
95	142	64	237	11	218	108	185	247	38	152	69	163	114	196	17
167	118	200	21	243	34	148	65	15	222	112	189	91	138	60	233
180	97	211	2	232	53	135	86	28	201	123	170	80	157	47	254
141	96	238	63	217	12	186	107	37	248	70	151	113	164	18	195
154	75	249	44	206	31	173	128	50	227	81	132	102	183	5	216

Example 6.2 (A family of bimagic squares of odd order.)
Take $R = \mathbb{Z}/q\mathbb{Z}$ with $q \geq 3$, q odd,

$$X = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 1 & 1 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{pmatrix},$$

$t \in R^4$ arbitrary and $N : R \to \{0, 1, \ldots, q-1\}$ the standard bijection (of type -1) as in 3.4. Then the corresponding $q^2 \times q^2$ matrices M as defined in theorem 2.2 are bimagic.

In particular this gives a family of bimagic squares of odd order.

1	35	60	23	48	79	18	40	65
70	14	39	56	9	31	78	19	53
49	74	27	44	69	10	30	61	5
38	72	13	33	55	8	52	77	21
26	51	73	12	43	68	4	29	63
59	3	34	81	22	47	64	17	42
75	25	50	67	11	45	62	6	28
36	58	2	46	80	24	41	66	16
15	37	71	7	32	57	20	54	76

Finally, if we choose $q = 3$ and $t = \begin{pmatrix} 2 & 1 & 2 & 0 \end{pmatrix}^t$ we recover the associative 9×9 bimagic square constructed by R.V. Heath (see p. 212 [2]) from before 1974.

Example 6.3 (An associative, pandiagonal, bimagic, ... magic square of order 25.) Take $R = \mathbb{F}_5$, $N : R \to \{0, 1, 2, 3, 4\}$ the standard bijection (of type -1) and

$$X = \begin{pmatrix} 1 & 1 & 2 & 2 \\ 1 & 2 & 2 & 4 \\ 1 & 3 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad t = \begin{pmatrix} 0 \\ 4 \\ 0 \\ 2 \end{pmatrix}.$$

Then the corresponding 25×25 matrix is associative, pandiagonal, bimagic and has the following properties:

i) Each of the 25 standard 5×5 submatrices is pandiagonal (even with the same magic sum).

ii) For each pair (i, j) $(1 \leq i, j \leq 25)$ the 5×5 matrix obtained by deleting each row with row number not equivalent to i mod 5 and each column with column number not equivalent to j mod 5 is pandiagonal!

103 350 567 164 381	291 513 235 452 74	584 176 423 20 362	147 494 86 308 530	440 32 254 621 218
167 389 106 328 575	460 52 299 516 238	23 370 587 184 401	311 533 130 497 94	604 221 443 40 257
331 553 175 392 114	524 241 463 60 277	187 409 1 373 595	480 97 319 536 133	43 265 607 204 446
400 117 339 556 153	63 285 502 249 466	351 598 195 412 9	544 136 483 80 322	207 429 46 268 615
564 156 378 125 342	227 474 66 288 510	420 12 359 576 198	83 305 547 144 486	271 618 215 432 29
134 476 98 320 537	447 44 261 608 205	115 332 554 171 393	278 525 242 464 56	591 188 410 2 374
323 545 137 484 76	611 208 430 47 269	154 396 118 340 557	467 64 281 503 250	10 352 599 191 413
487 84 301 548 145	30 272 619 211 433	343 565 157 379 121	506 228 475 67 289	199 416 13 360 577
526 148 495 87 309	219 436 33 255 622	382 104 346 568 165	75 292 514 231 453	363 585 177 424 16
95 312 534 126 498	258 605 222 444 36	571 168 390 107 329	239 456 53 300 517	402 24 366 588 185
290 507 229 471 68	578 200 417 14 356	141 488 85 302 549	434 26 273 620 212	122 344 561 158 380
454 71 293 515 232	17 364 581 178 425	310 527 149 491 88	623 220 437 34 251	161 383 105 347 569
518 240 457 54 296	181 403 25 367 589	499 91 313 535 127	37 259 601 223 445	330 572 169 386 108
57 279 521 243 465	375 592 189 406 3	538 135 477 99 316	201 448 45 262 609	394 111 333 555 172
246 468 65 282 504	414 6 353 600 192	77 324 541 138 485	270 612 209 426 48	558 155 397 119 336
441 38 260 602 224	109 326 573 170 387	297 519 236 458 55	590 182 404 21 368	128 500 92 314 531
610 202 449 41 263	173 395 112 334 551	461 58 280 522 244	4 371 593 190 407	317 539 131 478 100
49 266 613 210 427	337 559 151 398 120	505 247 469 61 283	193 415 7 354 596	481 78 325 542 139
213 435 27 274 616	376 123 345 562 159	69 286 508 230 472	357 579 196 418 15	550 142 489 81 303
252 624 216 438 35	570 162 384 101 348	233 455 72 294 511	421 18 365 582 179	89 306 528 150 492
597 194 411 8 355	140 482 79 321 543	428 50 267 614 206	116 338 560 152 399	284 501 248 470 62
11 358 580 197 419	304 546 143 490 82	617 214 431 28 275	160 377 124 341 563	473 70 287 509 226
180 422 19 361 583	493 90 307 529 146	31 253 625 217 439	349 566 163 385 102	512 234 451 73 295
369 586 183 405 22	532 129 496 93 315	225 442 39 256 603	388 110 327 574 166	51 298 520 237 459
408 5 372 594 186	96 318 540 132 479	264 606 203 450 42	552 174 391 113 335	245 462 59 276 523

More research into different properties and various examples can be found in the thesis of the second author ([6]). The reader is also referred to the website ([7]).

Acknowledgment: The authors like to thank Michiel de Bondt for various stimulating and helpful discussions.

References

[1] Gakuho Abe, *Unsolved problems on magic squares*, Discrete Mathematics 127 (1994) pp. 3-13

[2] W.W. Rouse Ball and H.S.M. Coxeter, *Mathematical Recreations and Essays*, 12^{th} edition 1974, Univ. of Toronto Press

[3] David S. Brée and Kathleen Ollerenshaw, *Most-perfect pandiagonal magic squares : their construction and enumeration*, Institute for Mathematics and its Applications, Southend-on-Sea, 1998, ISBN:0-905091-06-X

[4] Christian Boyer and André Viricel, *Les premiers carrés tétra et pentamagiques*, Pour la science, issue 286, pp. 98-102, August 2001

[5] Christian Boyer, website `http://www.multimagie.com`

[6] Christian Eggermont, Masters Thesis, Radboud University Nijmegen to appear.

[7] Christian Eggermont, `http://www.puzzled.nl`

[8] Pan Fengchu, Announcements at `http://www.zhghf.net/China/` and `http://www.zhghf.net/` (Chinese)

[9] Martin Gardner, *Magic Squares and Cubes* Ch.17 in *Time Travel and Other Mathematical Bewilderments*, New York: W.H. Freeman, pp.213-225, 1988

[10] Paul C. Pasles, *The Lost Squares of Dr. Franklin: Ben Franklin's Missing Squares and the Secret of the Magic Circle*, Amer. Math. Monthly 108, June-July 2001, pp. 489-511
See also the author's website: `http://www.pasles.org`

[11] G. Pfeffermann, *Les Tablettes du Chercheur, Journal des Jeux d'Esprit et de Combinaisons*, (fortnightly magazine) issues of 1891 Paris.

[12] Clifford A. Pickover, *The zen of magic squares, circles, and stars*, 2002, Princeton University press. ISBN: 0-691-07041-5

[13] Guenter Stertenbrink, `http://magictour.free.fr`, Announcement of August 5 2003.

[14] Ian Stewart, *Most-Perfect Magic Squares*, Scientific American vol. 281 (1999), nr. 5, p. 122

[15] Eric W. Weisstein, *Magic Cube*, From MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/MagicCube.html`

Harm Derksen
Dept. of Mathematics, Univ. of Michigan
East Hall, 530 Church Street
Ann Arbor, MI 48109-1043
hderksen@umich.edu

Christian Eggermont
Dept. of Mathematics, Univ. of Nijmegen
6525 ED Nijmegen, The Netherlands
C.Eggermont@science.ru.nl

Arno van den Essen
Dept. of Mathematics, Univ. of Nijmegen
6525 ED Nijmegen, The Netherlands
A.vandenEssen@science.ru.nl